



ALC Resource Matching & Referral Provincial Reference Model

Privacy Framework



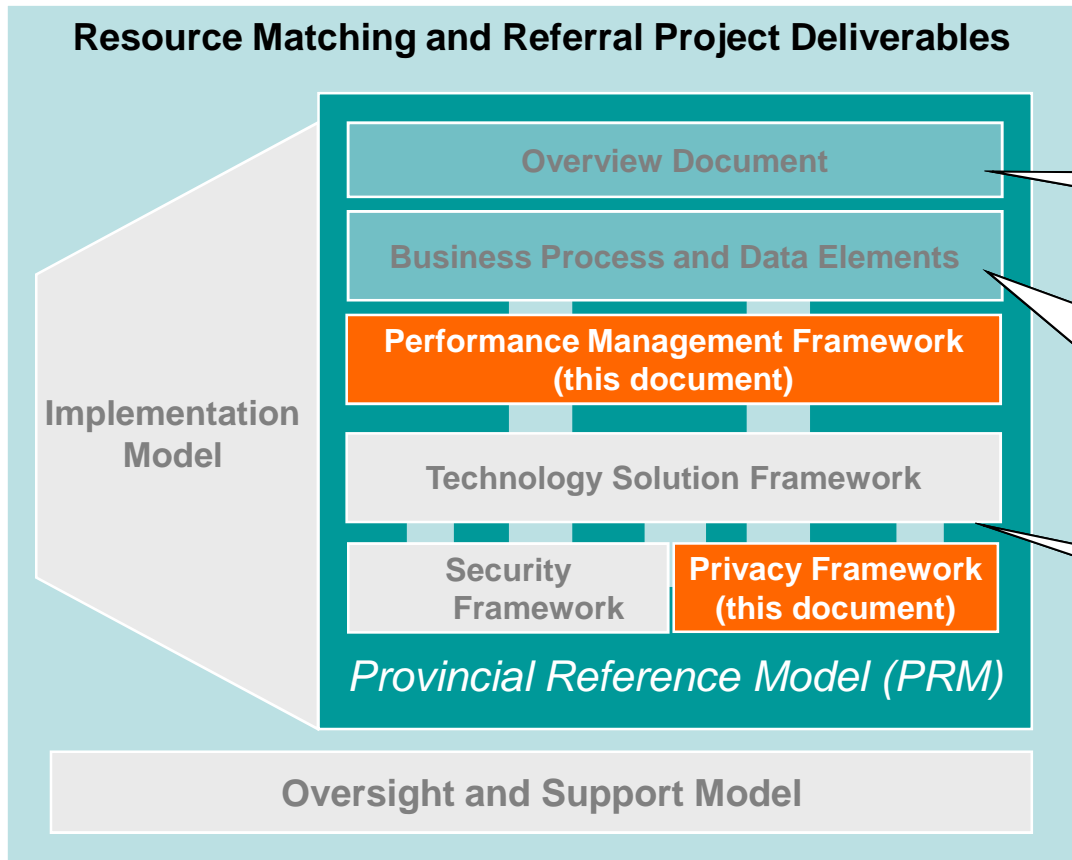
March 2010

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Summary of Privacy Analysis	Pages	13-15
• Privacy Background	Pages	17-25
– Privacy Framework	Page	17
– Support for eReferral Enablement	Page	18
– Guiding Principles	Page	19
– Key Assumptions	Pages	20-22
– Opportunities and Recommendations	Page	23-25
• Privacy Requirements	Pages	27-28
– RM&R Solution Privacy Requirements	Pages	27-28
• Appendices	Pages	30-31
– Appendix 1: Privacy Requirements	Pages	30
– Appendix 2: Approach	Pages	31

Orientation to the Provincial Reference Model (PRM) Deliverables

All work streams of the PRM are integrated and interdependent. As a result, it is recommended that the reader of this document should review other components of the PRM to ensure a comprehensive understanding of the privacy work stream.



In addition to this document, review the following for a comprehensive understanding of the Privacy Framework:

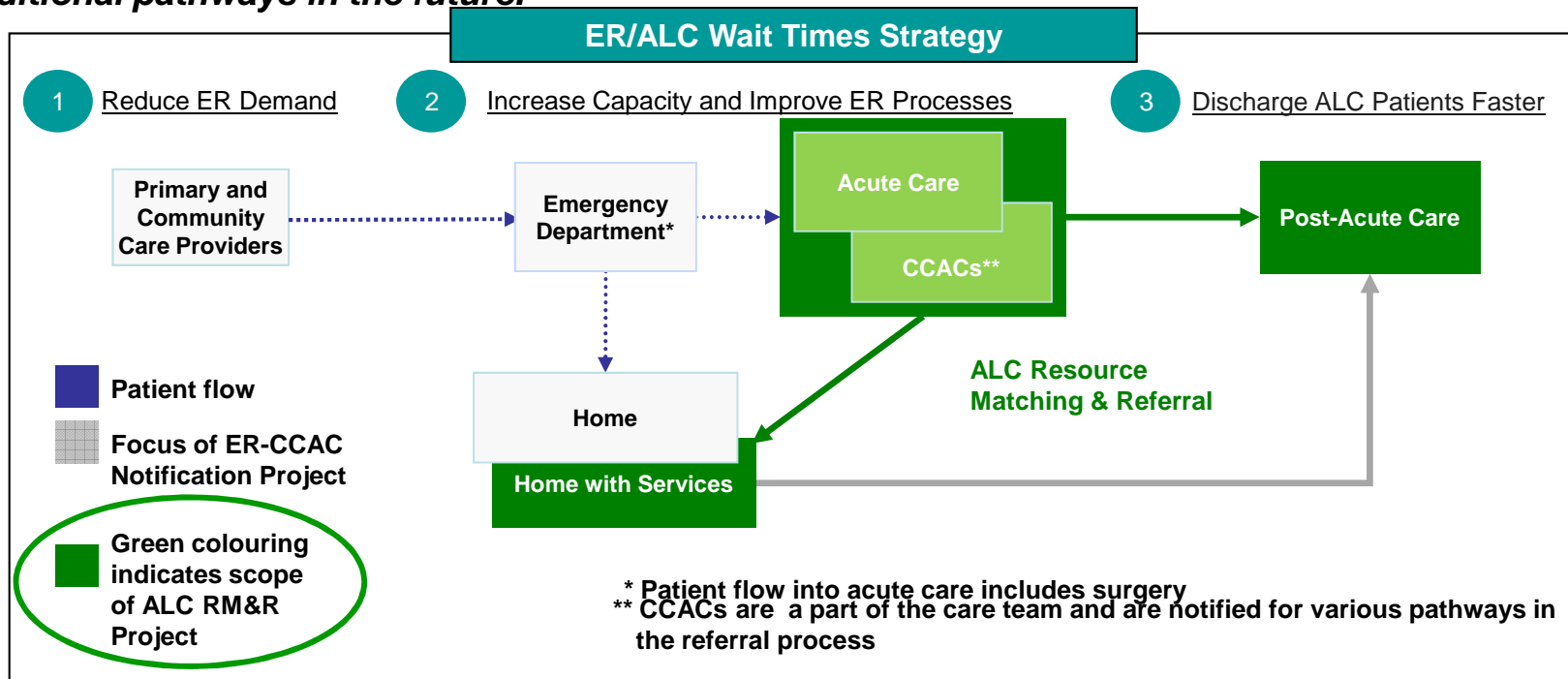
The **Overview Document** provides a detailed overview of the PRM.

In the **Business Process and Data Elements** document, the high-level business process determines which privacy roles are defined within a RM&R solution and the data elements identify what personal health information is collected and stored.

The **Technology Solution Framework** document outlines a conceptual RM&R architecture and this provides context for the application of Personal Health Information Protection Act (PHIPA) requirements.

Project Scope

The Alternate Level of Care (ALC) Resource Matching & Referral (RM&R) project focuses on referrals from the acute to post-acute setting for four specific pathways* and will serve as the foundation for additional pathways in the future.



The ALC RM&R project consists of four in-scope post-acute care destinations:

- Acute to Rehab
- Acute to Long-Term Care (LTC)
- Acute to Complex Continuing Care (CCC)
- Acute to In-Home Services

RM&R Project - Guiding Principles

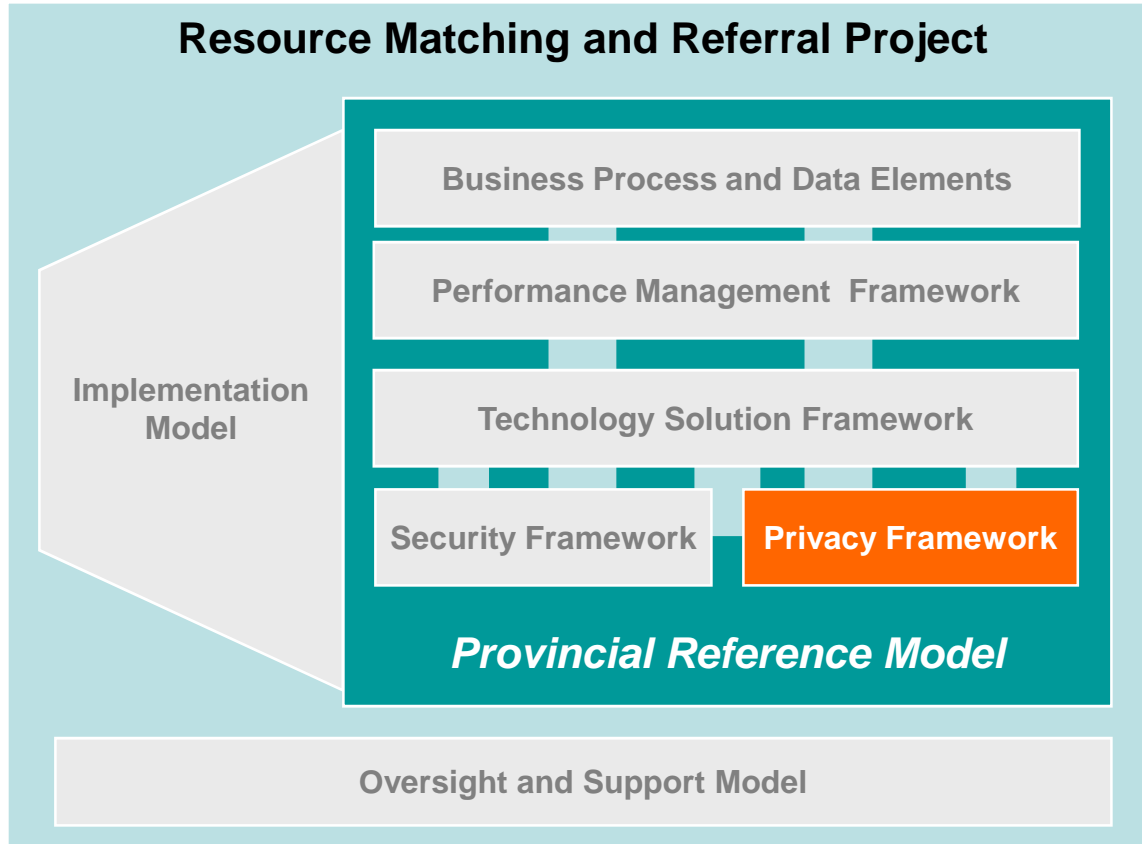
The following guiding principles have served as a foundation for the overall RM&R project.

RM&R Guiding Principles

<p>General</p>	<ul style="list-style-type: none"> • The PRM will be outcomes-focused, identifying “what” needs to occur, and leave the “who” and “how” to LHINs/LHIN clusters. • The PRM will not be tailored to a specific application, but will focus on the functionality required to support the future state of RM&R. • The outcome of this initiative will be focused on reducing the ALC component of patients’ wait times and increasing patient throughput; however, the model will also be flexible to adapt to other types of referrals over time.
<p>Implementation</p>	<ul style="list-style-type: none"> • LHINs will be accountable for implementation results. • LHINs/LHIN clusters will determine the most appropriate approach to implementation of RM&R solutions within their areas, including clustering and software selection. • LHINs must be aligned to the PRM as they implement RM&R solutions.

Objectives

The RM&R PRM includes five distinct components.* This document details the main recommendations from the privacy work stream.



The objectives of the privacy work stream are:

- To ensure the Alternate Level of Care (ALC) RM&R solution business processes and technical architecture comply with the Personal Health Information Protection Act (PHIPA) requirements
- To identify privacy opportunities that should be considered when implementing a RM&R solution along with recommendations and next steps

***The PRM is supported by the Implementation Model to enable LHINs to implement RM&R solutions as well as the internal Oversight and Support Model to support the ongoing RM&R project.**

Context for Understanding Privacy

Personal Health Information will be collected and stored in a RM&R solution and therefore the role of the organization that hosts or supports this solution must meet certain statutory requirements, as outlined in Personal Health Information Protection Act (PHIPA).

Context

- Privacy aspects outlined should be considered in the broader context of all components of the Provincial Reference Model: Business Process and Data Elements, Performance Management and Reporting Framework as well as the Technology and Security Frameworks.
- RM&R solutions must comply with the requirements that are outlined in this Privacy Framework and in PHIPA.
- In order for LHINs or LHIN clusters to be aligned to the PRM they must demonstrate that the RM&R solution complies with the privacy requirements outlined in the PRM at an appropriate stage in the implementation life cycle.
- Next Steps:
 - Consider privacy requirements during the design and implementation planning stage
 - Ensure that privacy expertise and a Privacy Impact Assessment (PIA) is conducted early in the implementation life cycle

Purpose of this document

Purpose

1. The purpose of this document is to describe the approach taken to establish a Privacy Framework and develop high-level privacy requirements for an Alternate Level of Care (ALC) Resource Matching and Referral (RM&R) solution.
2. In addition, this document provides Local Health Integration Network (LHIN) / Facility Privacy Officers and RM&R solution designers with a description of privacy roles, associated responsibilities and requirements that should be considered when implementing an ALC RM&R solution.

Methodology

- Understand ALC RM&R business processes and how personal health information (PHI) is used
- Understand how technology will be used to support the ALC RM&R business processes
- Determine what the privacy roles are within a RM&R solution
- Determine what privacy requirements should be addressed when implementing a RM&R solution

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Summary of Privacy Analysis	Pages	13-15
• Privacy Background	Pages	17-25
– Privacy Framework	Page	17
– Support for eReferral Enablement	Page	18
– Guiding Principles	Page	19
– Key Assumptions	Pages	20-22
– Opportunities and Recommendations	Page	23-25
• Privacy Requirements	Pages	27-28
– RM&R solution Privacy Requirements	Pages	27-28
• Appendices	Pages	30-31
– Appendix 1: Privacy Requirements	Pages	30
– Appendix 2: Approach	Pages	31

Executive Summary

The privacy components of the Provincial Reference Model provides an understanding for how privacy requirements were established and subject to the statutory framework for the RM&R solution.

Key Findings

- Due to the fact that the RM&R solution will access and transfer Personal Health Information (PHI), the solution is governed by PHIPA, the Ontario legislation which outlines the provisions for the collection, use and disclosure of PHI by Health Information Custodians (HICs).
- The PHIPA statutory authority for the operation of the proposed RM&R solution is that of a Health Information Network Provider (HINP). However, a PIA is required by all parties implementing a RM&R solution in order to analyze the individual design details for each LHIN cluster.
- A HINP is defined as a person who provides services to two or more Health Information Custodians (HICs), for the primary purpose of enabling the custodians to use electronic means to disclose Personal Health Information to one another.
- The HINP provision makes note of prescriptive measures, which must be in place to ensure compliance with the legislation.

Key Considerations

- In order to comply with PHIPA, the HINP for the RM&R solution must consider the requirements as documented in the Act (see PHIPA, 2004, O.Reg. 329/04 6(1-4))
- The party acting in the role of the HINP shall have an existing privacy compliance program in place at their organization and shall update any existing protocols in order to accommodate the new privacy role.
- All HICs utilizing the HINP shall have existing privacy protocols in place at their facility, which at a minimum, govern the collection, use and disclosure of PHI.
- LHINs or LHIN clusters are responsible for acquiring the appropriate privacy expertise in order to understand their statutory obligations and apply the privacy requirements for the implementation of a RM&R solution.

Executive Summary: Implications and Recommendations

The following are the key recommendations and implications to consider when applying the ALC RM&R Privacy Framework into a RM&R solution.

Theme	Recommendations and Implications
PHIPA Compliance	<ul style="list-style-type: none"> The PHIPA requirements noted on slides 27 and 28 are mandatory for persons who operate a HINP.
Privacy Focus	<ul style="list-style-type: none"> The focus of this work stream, its objectives and the associated privacy requirements are targeted at: <ul style="list-style-type: none"> Vendors and solution design teams who develop the system architecture The HINP who will adopt and manage the infrastructure of a RM&R solution
Privacy and the system development life cycle (SDLC)	<ul style="list-style-type: none"> Privacy and the protection of personal health information should be considered at every stage of the design and implementation life cycle in order to ensure compliance with the tenets of PHIPA.

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Summary of Privacy Analysis	Pages	13-15
• Privacy Background	Pages	17-25
– Privacy Framework	Page	17
– Support for eReferral Enablement	Page	18
– Guiding Principles	Page	19
– Key Assumptions	Pages	20-22
– Opportunities and Recommendations	Page	23-25
• Privacy Requirements	Pages	27-28
– RM&R solution Privacy Requirements	Pages	27-28
• Appendices	Pages	30-31
– Appendix 1: Privacy Requirements	Pages	30
– Appendix 2: Approach	Pages	31

Summary of Privacy Analysis (1 of 3)

The following are the key findings that were revealed during the privacy analysis of the high-level RM&R business process and conceptual architecture in the context of PHIPA

Key Findings (Operations Roles)

- LHIN Clusters
 - 14 LHINS will be divided into clusters
 - Each cluster will be made up of one or more LHINs
 - Each cluster will operate its own RM&R solution and either host the infrastructure services of the solution or outsource them to a third party

- Facilities (Hospitals)
 - Users of the RM&R solution
 - Use the solution to refer/accept patients to and from other ALC facilities
 - PHI will be transferred between facilities

Summary of Privacy Analysis (2 of 3)

The following are the key findings that were revealed during the privacy analysis of the high-level RM&R business process and conceptual architecture in the context of PHIPA.

Key Findings (Facilities)

- PHIPA regards facilities such as hospitals and Long -Term Care homes as Health Information Custodians (HICs) as noted in section 3(1) (4).
- A facility such as a hospital (HIC) will use the RM&R solution to submit the PHI of patients when processing a referral. The patients PHI will be transferred electronically to another facility (HIC) which will use this information to determine whether to accept or reject the referral.
 - Personal health information is defined in section 4(1) of the Act, which reads in part as follows:
 - In this Act, “personal health information”, subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information:
 - a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family,
 - b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual, ...
- PHI is being collected from individuals by the HICs for the purpose of submitting a referral to an ALC facility. This referral is made with the implied consent of the individual.
 - PHIPA ss. 29(a) states that: a health information custodian shall not collect, use or disclose personal health information about an individual unless it has the individual’s consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian’s knowledge, is necessary for a lawful purpose.

Summary of Privacy Analysis (3 of 3)

The following are the key findings that were revealed during the privacy analysis of the high-level RM&R business process and conceptual architecture in the context of PHIPA.

Key Findings (Statutory Authority for RM&R Solution Providers)

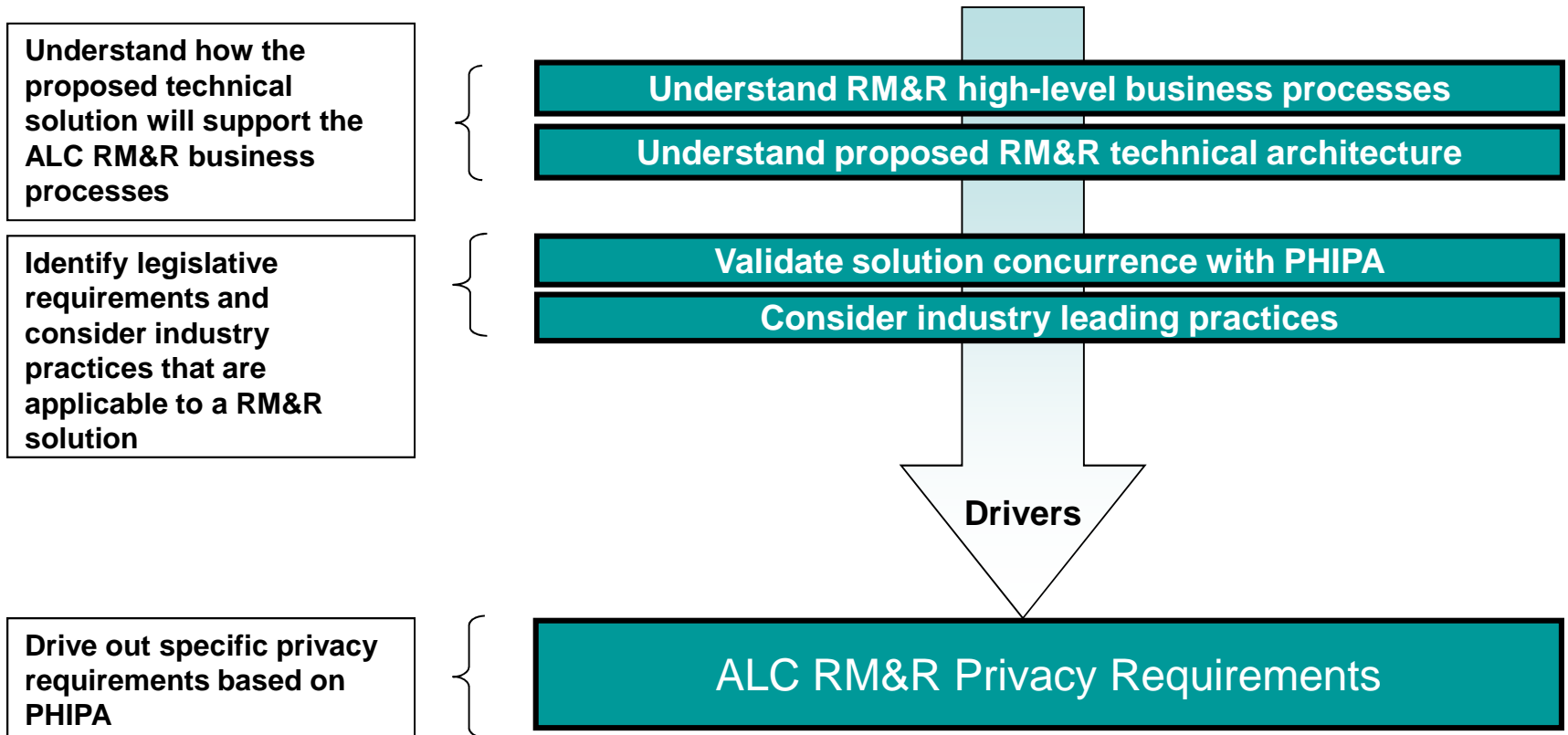
- PHIPA makes provisions for a HIC to use a health information network provider (HINP) to allow two or more HICs to use electronic means in order to exchange PHI.
- As part of the development of this project, each LHIN cluster has been tasked with providing a RM&R solution to facilitate patient referral.
- Therefore, LHIN clusters will be operating under the PHIPA statutory authority of a Health Information Network Provider (HINP).
- In order for LHINs to provide the HINP service, the prescribed requirements outlined in the PHIPA Regulation, section 6(3) must be applied to the RM&R solution.

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Summary of Privacy Analysis	Pages	13-15
• Privacy Background	Pages	17-25
– Privacy Framework	Page	17
– Support for eReferral Enablement	Page	18
– Guiding Principles	Page	19
– Key Assumptions	Pages	20-22
– Opportunities and Recommendations	Page	23-25
• Privacy Requirements	Pages	27-28
– RM&R solution Privacy Requirements	Pages	27-28
• Appendices	Pages	30-31
– Appendix 1: Privacy Requirements	Pages	30
– Appendix 2: Approach	Pages	31

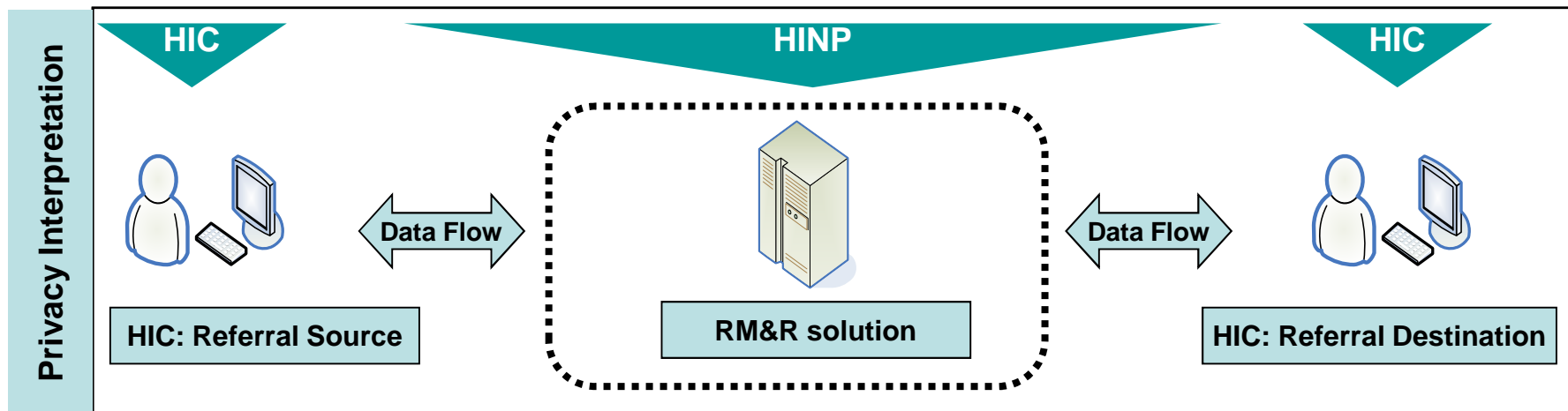
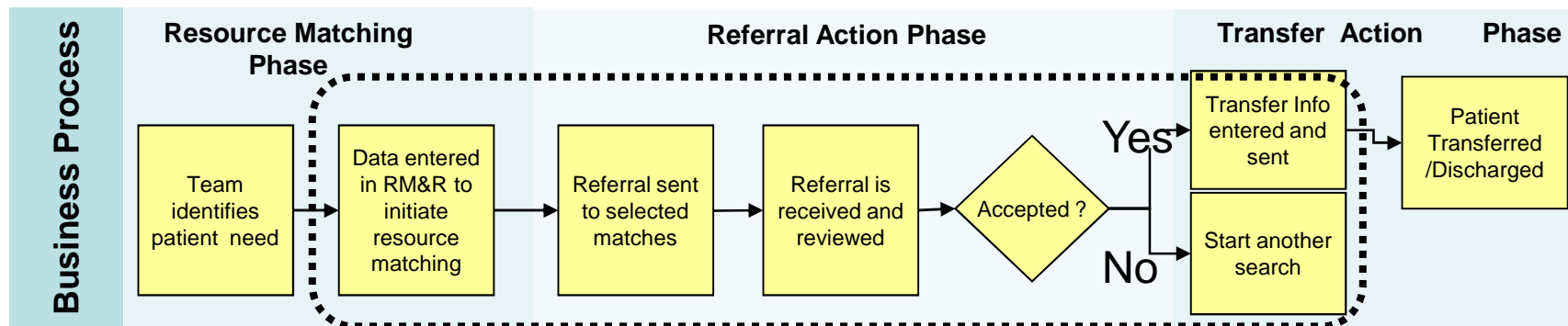
Privacy Framework

The ALC RM&R Privacy Framework was designed to outline PHIPA privacy requirements for LHINs or LHIN clusters to consider when implementing a RM&R solution.



Support for eReferral Process Enablement

The Privacy Framework interprets ALC RM&R business processes according to PHIPA authorities by identifying the privacy roles and how PHI will be used in these roles. Once the roles have been identified, privacy requirements that are applicable to a HINP are addressed to ensure compliance.



Guiding Principles

The following guiding principles were used to shape the work of the privacy work stream.

Guiding Principles	
Legislative Requirements	▪ Identify applicable privacy requirements that are prescribed in PHIPA
	▪ Apply privacy legislation to derive a set of ALC RM&R privacy requirements
Industry Leading Practices	▪ Consideration was given to leading privacy practices

Key Assumptions

The privacy component of the PRM has been defined in the context of the following key assumptions:

1. Hospitals and other participating health care facilities (i.e. Health Information Custodians) are expected to have well established privacy processes, procedures, guidelines and a governance structure that support existing systems which house PHI. At a minimum, this should include:

Accountability

- a. A privacy program that describes how the organization collects, uses and discloses PHI
- b. Supporting procedures for PHI breach management, access management, inquiries, complaint management and consent management
- c. Privacy contacts at each hospital/facility
- d. Privacy training for staff

Identifying Purpose

- a. The provision of notices that describe why the organization collects PHI

Consent

- a. Consent policies and procedures which provide an overview of the different types of consent and how a hospital or facility manages a patient's consent (consent in the RM&R solution is implied and managed between the practitioner and patient; the RM&R solution will manage the withdrawal of consent)

Key Assumptions (2 of 3)

The privacy component of the PRM has been defined in the context of the following key assumptions:

Limiting Collection

- a. A policy or procedure to review data elements to ensure that the organization collects only data elements that are required to fulfill an identified purpose

Limiting Use, Disclosure and Retention

- a. Conducting regular reviews to ensure that access to PHI is granted on a “need-to-know” basis
- b. Policies and procedures to manage PHI disclosure
- c. A Data Retention policy

Accuracy

- a. A Data Quality program
- b. A resource who performs a data steward function
- c. A procedure to access and correct data

Safeguards

- a. Physical Safeguards, such as access cards to protect areas where PHI is viewed or accessed
- b. Administrative safeguards, such as confidentiality agreements, privacy training & awareness and threat risk assessments

Key Assumptions (3 of 3)

The privacy component of the PRM has been defined in the context of the following key assumptions:

Openness

- a. Policies and procedures to manage privacy inquiries and complaints
- b. A resource who acts as a privacy contact person to the public
- c. The availability of contact information for the organization's Privacy Office

Individual Access

- a. A procedure to access and correct data

Challenging Compliance

- a. The availability of the contact information of the organization's privacy officer
- b. A procedure to manage a privacy breach

2. LHINs or LHIN clusters are responsible for acquiring the appropriate privacy expertise in order to understand their statutory obligations and apply the privacy requirements for the implementation of a RM&R solution.

Opportunities and Recommendations (1 of 3)

The following opportunities, relative to the desired future state, have been identified along with suggested recommendations and next steps.

Opportunity	Recommendation	Next Steps
<ul style="list-style-type: none"> Ensure that use of external PHI data repositories into the health information network must be in compliance with PHIPA 	<ul style="list-style-type: none"> Conduct a privacy authority review for any material changes to the RM&R solution 	<ul style="list-style-type: none"> Embed a privacy gate into the development of any change management protocols for the RM&R solution
<ul style="list-style-type: none"> Ensure that HINP processes and the technical solution must be flexible enough to deal with the issue of withdrawal of consent and patient initiated access restrictions (blocking forms) 	<ul style="list-style-type: none"> Ensure that any Request for Proposal (RFP) or system design includes consent management provisions as outlined in item 20.12. of the detailed requirements Where consent is managed through a manual process, ensure that HIC policies reflect the process that should be followed for withdrawn or limited consent 	<ul style="list-style-type: none"> Ensure that potential RM&R solution vendors and/or design teams are aware of all consent requirements and ensure that they are addressed

Opportunities and Recommendations (2 of 3)

The following opportunities, relative to the desired future state, have been identified along with suggested recommendations and next steps.

Opportunity	Recommendation	Next Steps
<ul style="list-style-type: none"> Ensure that privacy assessments are conducted when interoperability is enabled between LHIN or LHIN cluster RM&R solutions across the province 	<ul style="list-style-type: none"> Written agreements between facilities and health information network providers should include a provision for the sharing of PHI with other clusters, within Ontario, who are part of the RM&R PRM project 	<ul style="list-style-type: none"> When interoperability between RM&R solutions is implemented, LHINs involved should ensure that appropriate written agreements are in place to address PHI

Opportunities and Recommendations (3 of 3)

The following opportunities, relative to the desired future state, have been identified along with suggested recommendations and next steps.

Opportunity	Recommendation	Next Steps
<ul style="list-style-type: none"> ▪ Ensure that privacy assessments are conducted when contemplating the outsourcing of infrastructure services that will support a RM&R solution 	<ul style="list-style-type: none"> ▪ An organization that provides infrastructure services for the RM&R solution on behalf of a LHIN cluster should meet the following requirements: <ul style="list-style-type: none"> ▪ The organization shall adopt all RM&R HINP requirements . ▪ The LHIN cluster should ensure robust privacy provisions are included in all contractual agreements with the organization. ▪ The LHIN cluster should ensure PHI is stored in Canada 	<ul style="list-style-type: none"> ▪ Ensure a PIA is conducted which examines the privacy risks of a third party infrastructure provider for the RM&R solution ▪ Include privacy provisions which outline the service providers restrictions on the collection, use, disclosure, storage, retention and destruction of PHI
<ul style="list-style-type: none"> ▪ LHIN clusters must ensure that they adopt a standard privacy document management practice 	<ul style="list-style-type: none"> ▪ Promote the standardized use of documents to promote consistent leading practices and minimize duplication and re-work across LHINs. 	<ul style="list-style-type: none"> ▪ The RM&R project team to work with key stakeholders to provide examples of documents including, but not limited to: <ul style="list-style-type: none"> ▪ HINP Privacy Policy and Procedures ▪ License Agreements ▪ Data Sharing Agreements ▪ Sample privacy provisions for contracts ▪ PIA guidelines

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Summary of Privacy Analysis	Pages	13-15
• Privacy Background	Pages	17-25
– Privacy Framework	Page	17
– Support for eReferral Enablement	Page	18
– Guiding Principles	Page	19
– Key Assumptions	Pages	20-22
– Opportunities and Recommendations	Page	23-25
• Privacy Requirements	Pages	27-28
– RM&R solution Privacy Requirements	Pages	27-28
• Appendices	Pages	30-31
– Appendix 1: Privacy Requirements	Pages	30
– Appendix 2: Approach	Pages	31

RM&R solution Privacy Requirements (1 of 2)

This slide and the following one provides a list of HINP privacy requirements and constraints that should be followed when implementing a RM&R solution. These requirements are derived from PHIPA and privacy best practices.

Number	Privacy Principle	Requirement / Constraint	Addressed (A)dmistratively or (T)echnically
20.1	Accountability	The HINP shall appoint an individual, such as a privacy officer, to be responsible for privacy matters.	<ul style="list-style-type: none"> • (A) Appoint a person to act as a privacy officer
20.2	Accountability/Openness	The HINP must provide to the public a description of services, safeguards, directives, guidelines and policies. (see section 6(3), 3. PHIPA, 2004 – O.Reg. 329/04).	<ul style="list-style-type: none"> • (A) Create a privacy policy that contains general information on technical and administrative safeguards for protecting PHI
20.3	Accountability	The RM&R solution must have audit logging capabilities. (see section 6(3), 4. PHIPA, 2004 – O.Reg. 329/04).	<ul style="list-style-type: none"> • (T) Please see the Auditing security requirements 21.16 – 21.22 on page 18 of the Security Component of the Provincial Reference Model
20.4	Accountability	The HINP shall create an access role within the RM&R solution that has the ability to execute and view privacy reports generated by the solution. (see section 6(3), 4. PHIPA, 2004 – O.Reg. 329/04).	<ul style="list-style-type: none"> • (A) Develop an “audit log request procedure” that will describe how each HIC can view audit logs via the RM&R solution
20.5	Accountability	The HINP must provide HICs with a Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA) for the RM&R solution. (see section 6(3), 5. PHIPA, 2004 – O.Reg. 329/04).	<ul style="list-style-type: none"> • (A) Conduct a Privacy Impact Assessment • (A) Conduct a Threat Risk Assessment
20.6	Safeguards	The HINP must provide HICs with a plain language description of the services and safeguards that it provides. (see section 6(3), 2. PHIPA, 2004 – O.Reg. 329/04).	<ul style="list-style-type: none"> • (A) Develop a general policy statement that describes: <ul style="list-style-type: none"> – The services the HINP provides to the HICs – The safeguards that are present in the RM&R solution
20.7	Use, Disclosure and Retention of PHI	The HINP shall implement policies and procedures to appropriately control access of employees and third parties that support the RM&R solution. (see section 6(3), 6. PHIPA, 2004 – O.Reg. 329/04).	<ul style="list-style-type: none"> • (A) Develop a privacy training and awareness procedure • (A) Track completion of training, e.g. use a Privacy Acknowledgement Signoff form

RM&R solution Privacy Requirements (2 of 2)

This slide provides a list of HINP privacy requirements and constraints that should be followed when implementing a RM&R solution. These requirements are derived from PHIPA and privacy best practices.

Number	Privacy Principle	Requirement / Constraint	Addressed (A)dministratively or (T)echnically
20.8	Use, Disclosure and Retention of PHI	The HINP must enter into a written agreement with each HIC with respect to services and safeguards. (see section 6(3), 7. PHIPA, 2004 – O.Reg. 329/04).	<ul style="list-style-type: none"> • (A) Develop / execute an agreement with each HIC
20.9	Use, Disclosure and Retention of PHI	The RM&R solution shall support the ability to restrict access to PHI from HICs when access to that information is no longer required by a HIC for referral processing.	<ul style="list-style-type: none"> • (A) Ensure that referral data retention is consistent with HIC retention policy for comparable solutions that maintain PHI
20.10	Use, Disclosure and Retention of PHI	The HINP must notify every applicable HIC, at the first reasonable opportunity, of any breach related to the unauthorized access, use, disclosure or disposal of PHI. (see section 6(3), 1. PHIPA, 2004 – O. Reg. 329/04).	<ul style="list-style-type: none"> • (A) Develop a breach management process for identifying, managing and resolving privacy breaches
20.11	Use, Disclosure and Retention of PHI	The RM&R solution shall not disclose PHI to other external sources other than HICs that are part of the RM&R solution (see section 6(1), 2. PHIPA, 2004 – O. Reg. 329/04).	<ul style="list-style-type: none"> • (T) Conduct a privacy review to ensure that ALC RM&R participants are properly defined from a privacy and legal perspective
20.12	Consent	The RM&R solution must support the following consent requirements: <ul style="list-style-type: none"> • Ability to record a patients request to withdraw their participation in the program 	<ul style="list-style-type: none"> • (T) (A) Ensure solution design and operational processes allow for deletion of patient's information from the RM&R solution if they withdraw from participation in the program

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Summary of Privacy Analysis	Pages	13-15
• Privacy Background	Pages	17-25
– Privacy Framework	Page	17
– Support for eReferral Enablement	Page	18
– Guiding Principles	Page	19
– Key Assumptions	Pages	20-22
– Opportunities and Recommendations	Page	23-25
• Privacy Requirements	Pages	27-28
– RM&R solution Privacy Requirements	Pages	27-28
• Appendices	Pages	30-31
– Appendix 1: Privacy Requirements	Pages	30
– Appendix 2: Approach	Pages	31

Appendix 1: Privacy Requirements

- Detailed Privacy Requirements are available as a separate attachment.

Requirements (PDF):

ALC RMR Glossary, Functional and Non-Functional Requirements Approved Dec 2009.pdf

Appendix 2: Privacy Work Stream Approach

- The ALC RM&R project team established a Business Process & Data Elements Sub-group that was composed of representatives from across the health care spectrum in Ontario.
- This sub-group was tasked with developing consensus on the ALC RM&R high-level business process flows and data elements.
- The ALC RM&R project team also established a Technology Sub-group that was composed of health care technology specialists from across the province.
- The Technology Sub-group was tasked with developing consensus on a conceptual architecture that would support the RM&R business process.
- The ALC RM&R Privacy team members used PHIPA to develop a set of Privacy requirements that a HINP must implement in order to operate the RM&R solution, within the boundaries of the statute.