



ALC Resource Matching & Referral Provincial Reference Model *Security Framework*

March 2010

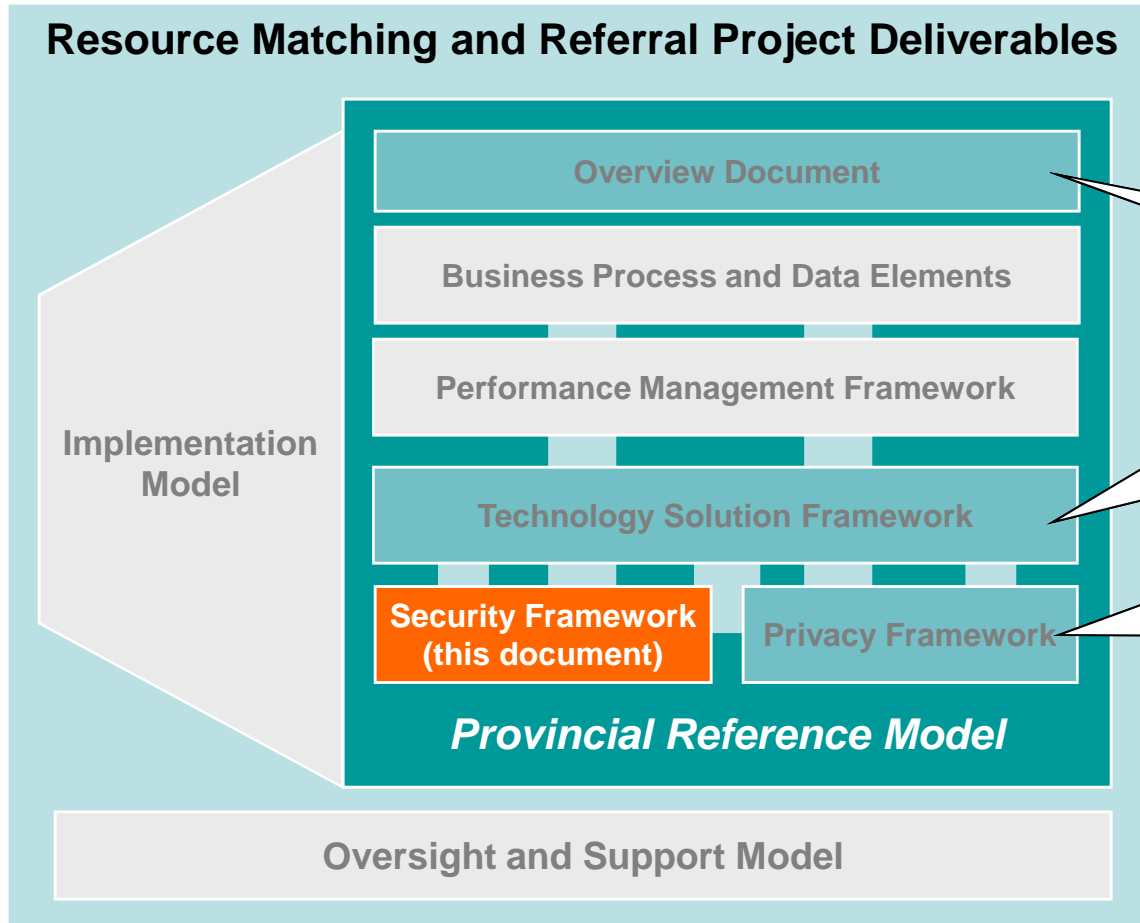


Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Security Background	Pages	13-16
– RM&R Security Framework	Page	13
– Security Guiding Principles	Page	14
– Key Assumptions	Page	15
– Opportunities and Recommendations	Page	16
• Security Requirements and Leading Practices	Pages	18-31
– Security Support for eReferral Process Enablement	Page	18
– Privacy Legislation and Security Requirements	Page	19
– RM&R Solution Security Requirements	Pages	20-25
– RM&R Operational Security Leading Practices	Pages	26-31
• Appendices	Pages	33-34
– Appendix 1: Security Requirements (Excel)	Page	33
– Appendix 2: Approach	Page	34

Orientation to the Provincial Reference Model (PRM) Deliverables

All components 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 security component.



In addition to this document, review these documents for a comprehensive understanding of the Security Framework:

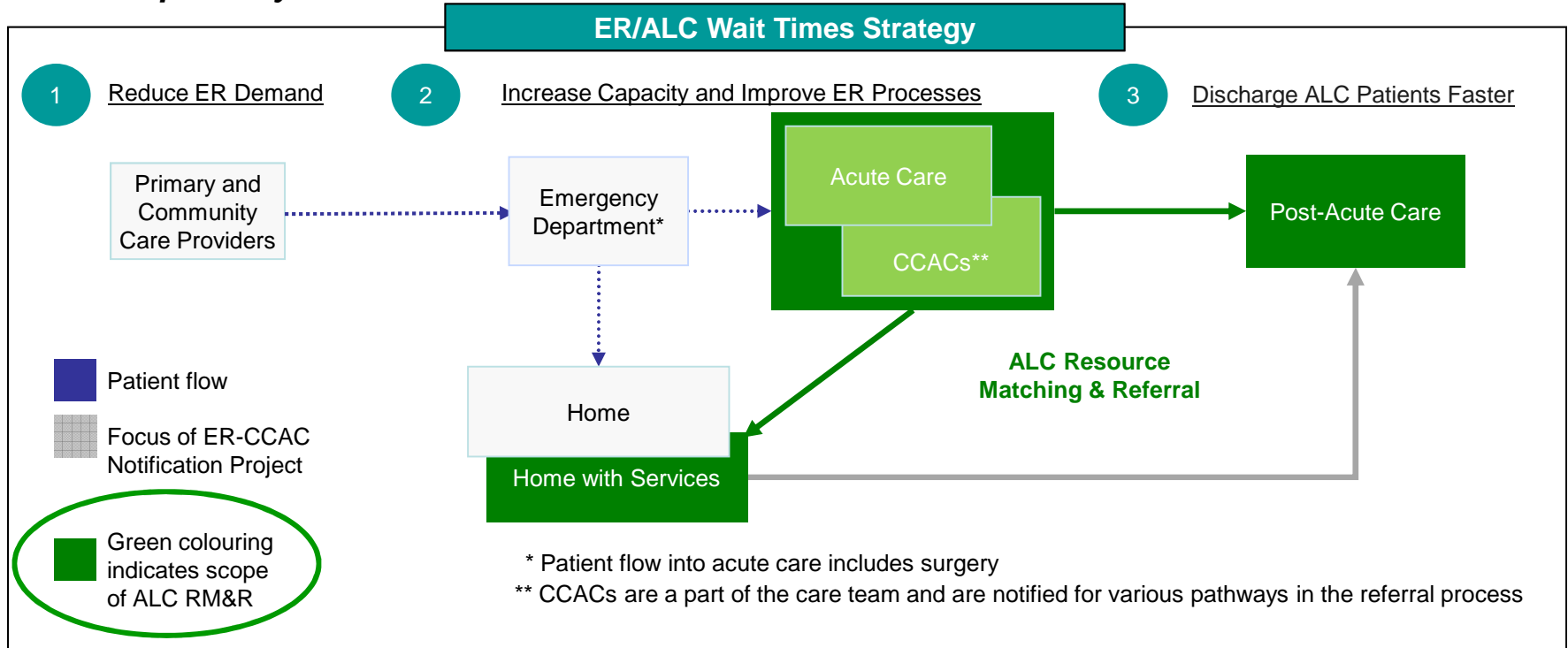
The **Overview Document** provides a detailed overview of the PRM.

The security requirements are addressed in the context of the RM&R conceptual architecture that is defined in the **Technology Solution Framework**.

The Privacy requirements in the **Privacy Framework** are based on the Personal Health Information Protection Act (PHIPA) and are the driver for some of the security 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

General

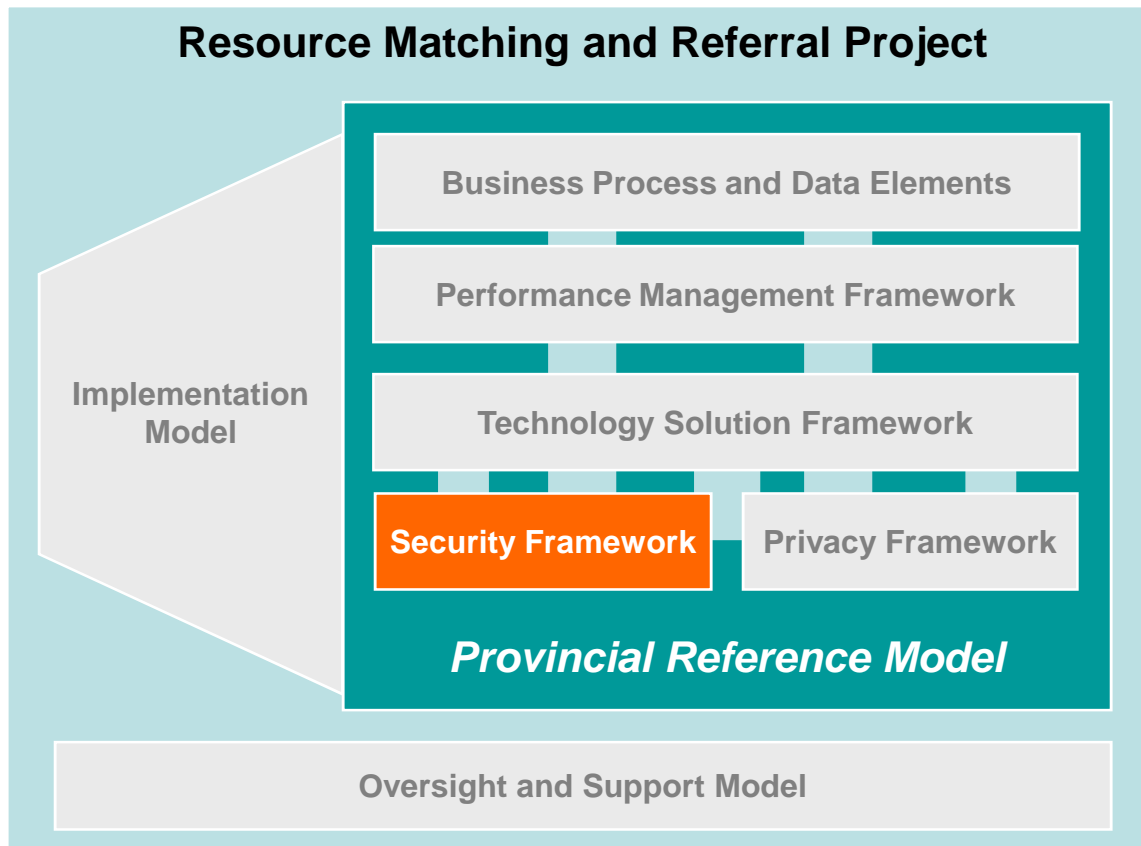
- The PRM will be outcomes-focused, identifying “what” needs to occur, and leave the “who” and “how” to LHINs/LHIN clusters.
- The PRM will not be tailored to a specific application, but will focus on the functionality required to support the future state of RM&R.
- The outcome of this initiative will 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.

Implementation

- 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 security component.



The objectives of the Security Framework are:

- To determine security requirements from legislation (PHIPA) that should be implemented as part of a RM&R solution.
- To determine how industry standards and leading practices should be incorporated into a RM&R solution.
- To develop a framework to drive out security requirements and align with the overall conceptual architecture of a RM&R solution.
- To suggest an approach for managing security risks and gaps.

***The PRM is supported by an Implementation Model to enable LHINs to implement RM&R solutions and an Oversight and Support Model for the RM&R project.**

Context for Understanding Security

The Security Framework, which is one aspect of the ALC RM&R Provincial Reference Model, provides a set of requirements and leading practices that LHINs must consider when procuring and implementing a RM&R solution.

Context

- Security aspects outlined should be considered in the broader context of all components of the PRM: Business Process and Data Elements, Performance Management Framework, as well as the Technology and Privacy Frameworks.
- RM&R solutions must conduct a gap analysis with the requirements that are outlined in this Security Framework.
- RM&R solutions must consider security leading practices that are presented in this Security Framework.
- Next Steps:
 - Commit to conducting a security assessment / threat risk assessment (TRA) and gap analysis of solution against RM&R provided security requirements during the early planning stage.
 - Ensure the availability of resources with security expertise in order to understand requirements and leading practices.

Purpose of this Document

Purpose

1. Describe the Security Framework used to develop high-level security requirements for a RM&R solution. This security framework will enable LHINs to define reasonable security requirements to implement a RM&R solution and meet regulatory obligations outlined in PHIPA.
2. Communicate security requirements to facilitate procurement and illustrate how they align with the RM&R conceptual architecture model.
3. Communicate operational security leading practices that will help LHINs operationalize and run a RM&R solution.

Methodology

- Investigate how privacy legislative requirements should be interpreted and adapted to a RM&R solution.
 - PHIPA
- Investigate and determine how industry standards and leading practices should be incorporated into a RM&R solution.
 - International Organization for Standardization (ISO) 27001 / 27002 / 27799
 - National Institute of Standards and Technology (NIST)
 - Federal Information Processing Standard (FIPS)
- Develop a set of security requirements and leading practices and guidelines that align with the overall conceptual technical architecture of a RM&R solution.
- Provide guidance on managing the risk associated with the gaps in the implementation of security requirements.

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Security Background	Pages	13-16
– RM&R Security Framework	Page	13
– Security Guiding Principles	Page	14
– Key Assumptions	Page	15
– Opportunities and Recommendations	Page	16
• Security Requirements and Leading Practices	Pages	18-31
– Security Support for eReferral Process Enablement	Page	18
– Privacy Legislation and Security Requirements	Page	19
– RM&R Solution Security Requirements	Pages	20-25
– RM&R Operational Security Leading Practices	Pages	26-31
• Appendices	Pages	33-34
– Appendix 1: Security Requirements (Excel)	Page	33
– Appendix 2: Approach	Page	34

Executive Summary

The RM&R Security Framework provides LHINs with a tool to define reasonable security requirements that meet regulatory obligations and follow industry leading practices.

Framework

- The ALC RM&R project team created a security framework in order to provide security guidance for LHINs implementing a RM&R solution. This framework was based on legislative requirements and industry leading practices, which in combination provide the driver for RM&R security requirements.
- The security requirements are divided into two broad categories:
 - Requirements that should be incorporated into a RM&R solution
 - Leading practices that should be considered in the operational aspects of a RM&R solution

Key Considerations

- In order to ensure the implementation of reasonable security controls within a RM&R solution, key items to consider are:
 - Using the supplied Security Framework to ensure comprehensive coverage of security considerations
 - Incorporating the RM&R solution security requirements into the Request for Proposal (RFP) for a RM&R solution
 - Incorporating the RM&R infrastructure security requirements when designing the solution infrastructure
 - Incorporating the RM&R operational security leading practices when operationalizing the RM&R solution
 - Conducting a TRA to identify gaps and residual risks

Executive Summary - Implications and Recommendations

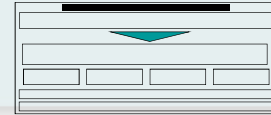
The following are key recommendations and implications to consider when utilizing the RM&R Security Framework:

Theme	Recommendations and Implications
Legislative Requirements	<ul style="list-style-type: none"> Regulatory requirements are not prescriptive with respect to security. This requires elaboration to determine what constitutes reasonable security and leading practices.
Industry Standards and Leading Practices	<ul style="list-style-type: none"> A broad range of standards and leading practices were considered, including Cancer Care Ontario (CCO) practice utilized for similar initiatives, provincial standards (e.g. Ontario Health Informatics Standards Committee (OHISC) Secure Toolkit; International Publications: NIST, ISO 27001 / 27002 / 27799, FIPS.)
Non-Prescriptive	<ul style="list-style-type: none"> The RM&R security requirements are stated in a manner that avoids being overly prescriptive yet are detailed enough that they provide value in the planning for the procurement and implementation of a RM&R solution.
Risk Management	<ul style="list-style-type: none"> Implement suggested RM&R solution security requirements, leading practices and apply risk management in order to achieve reasonable assurances that personal health information is appropriately protected.

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Security Background	Pages	13-16
– RM&R Security Framework	Page	13
– Security Guiding Principles	Page	14
– Key Assumptions	Page	15
– Opportunities and Recommendations	Page	16
• Security Requirements and Leading Practices	Pages	18-31
– Security Support for eReferral Process Enablement	Page	18
– Privacy Legislation and Security Requirements	Page	19
– RM&R Solution Security Requirements	Pages	20-25
– RM&R Operational Security Leading Practices	Pages	26-31
• Appendices	Pages	33-34
– Appendix 1: Security Requirements (Excel)	Page	33
– Appendix 2: Approach	Page	34

RM&R Security Framework



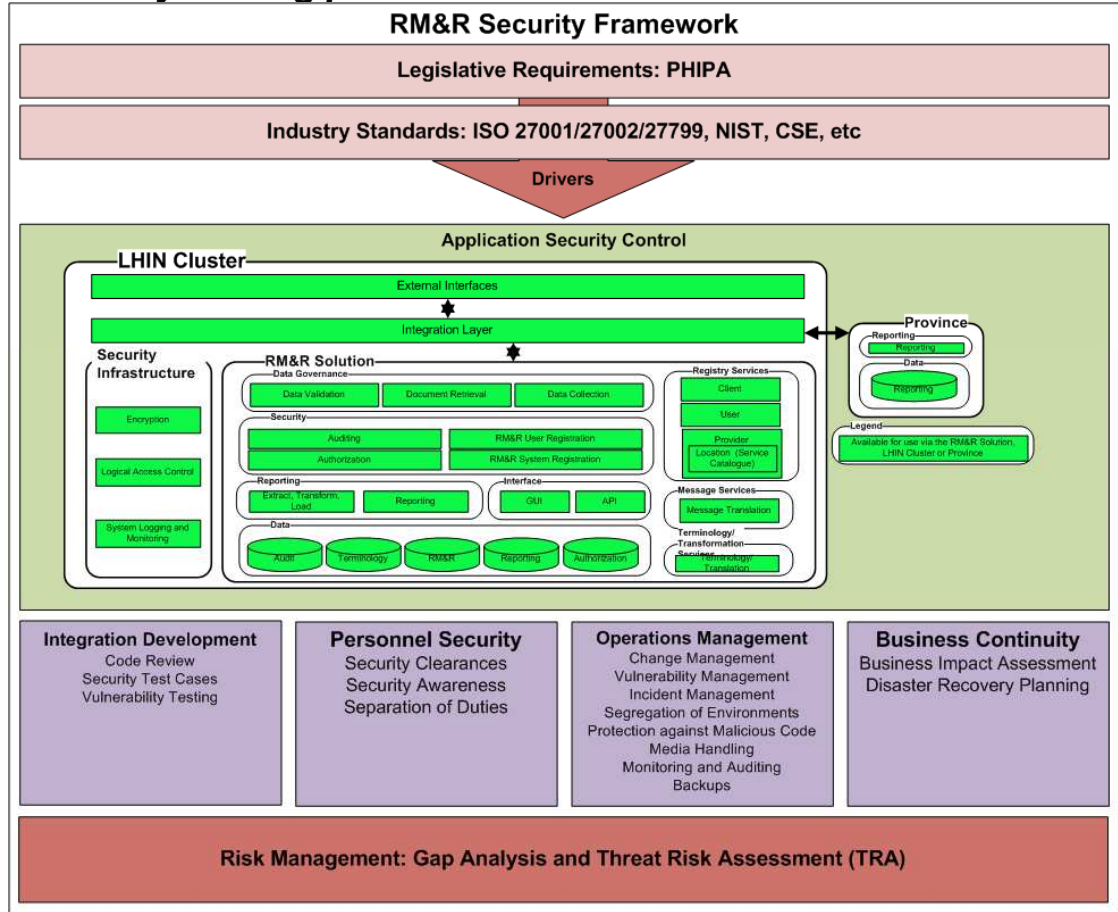
The RM&R Security Framework was designed to assist LHINs in developing reasonable security requirements to procure and implement a RM&R solution that meets regulatory obligations (i.e. PHIPA) and follows industry leading practices.

Identify legislative requirements and leading industry practices

Identify security requirements to facilitate procurement and design
 Illustrate how the requirements align with the RM&R conceptual architecture model

Identify operational security leading practices

Provide risk management guidance



Guiding Principles

The following guiding principles were used to shape the work of the security component:

Guiding Principles	
Legislative Requirements	▪ Identify requirements that are prescribed in privacy legislation (PHIPA)
	▪ Apply legislation to security requirements
Industry Standards and Leading Practices	▪ Identify leading security practices used at CCO for similar solutions
	▪ Identify provincial security standards, e.g. OHISC Secure Toolkit
	▪ Identify applicable industry security standards: ISO 27001 / 27002 / 27799; NIST; FIPS
Non-Prescriptive	▪ Strike a balance between providing actionable security guidance, while not being overly prescriptive, which will allow LHINs the flexibility to implement security measures, as appropriate for their business practices
Risk Management	▪ Conduct a Threat and Risk Assessment to identify gaps and residual risks

Key Assumptions

The security component of the PRM has been defined for LHIN / LHIN clusters in the context of the following key assumptions. LHINs or LHIN clusters are responsible for:

- Ensuring compliance with applicable (local or provincial) information security policies and standards
- Ensuring the Privacy Impact Assessment (PIA) and TRA are done at appropriate points during a RM&R solution implementation
- Acquiring the appropriate security expertise in order to understand and apply security controls, requirements and guidelines for the implementation of a RM&R solution
- Ensuring outsourced solutions will provide evidence that they satisfy required security objectives (as outlined in the framework). Specific security requirements will be documented and monitored in contracts and Service Level Agreements
- Assessing the applicability of requirements and recommendations to their specific solution. Not all recommendations will be applicable to all solutions
- Ensuring that appropriate security operational procedures (e.g. incident response, vulnerability management) are in place to manage and operate a RM&R solution
- Having a security program that will enable the implementation and maintenance of requirements and directives outlined in the RM&R Security Framework
- Considering physical security, however this is not in-scope of the RM&R Security Framework

Note: LHINs or LHIN clusters are not responsible for the security of Health Information Custodian environments, as this is not in-scope of the RM&R Security Framework.

Opportunities and Recommendations

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

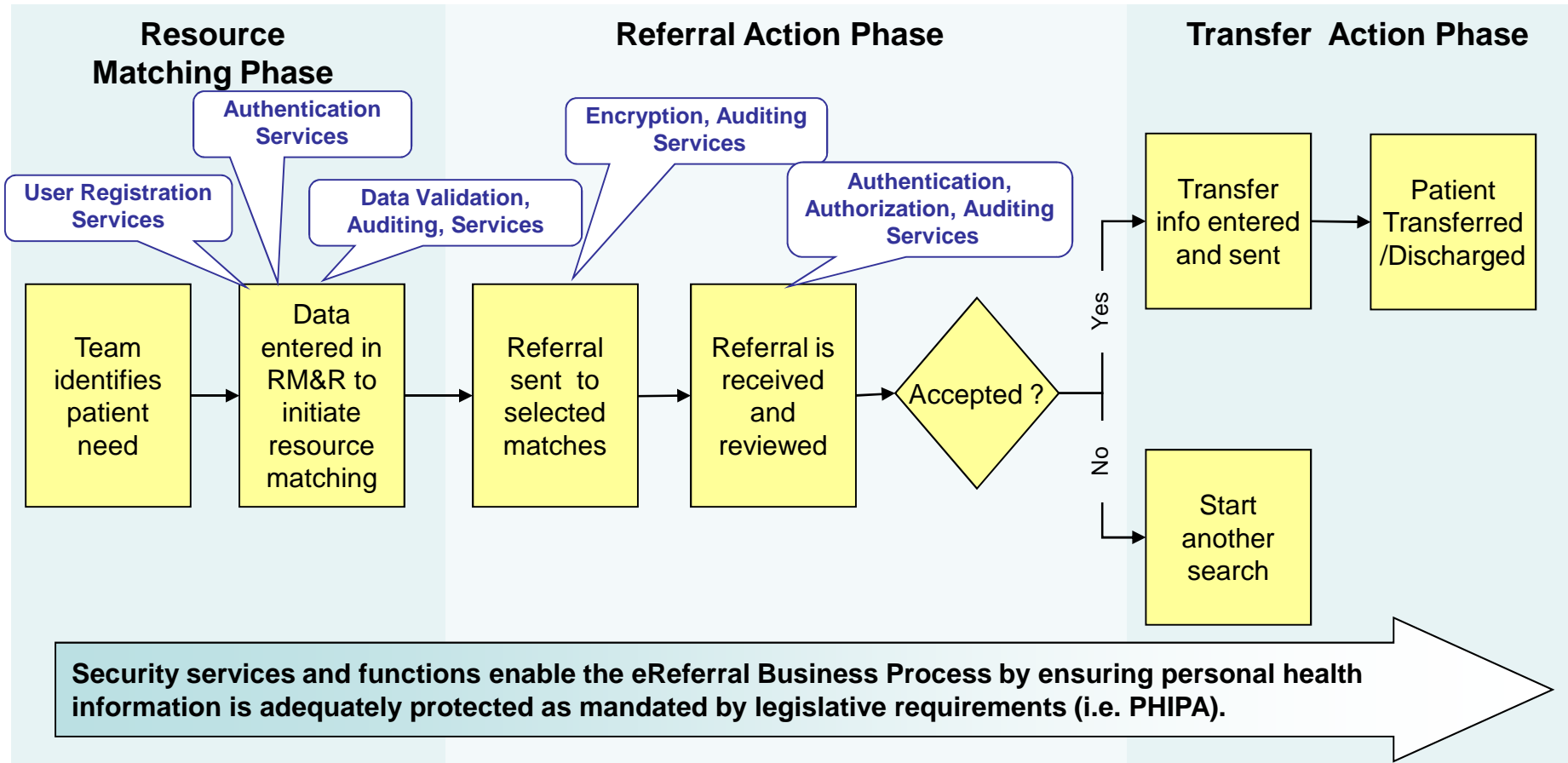
Opportunity	Recommendation	Next Steps
Ensure that LHINs have security expertise to perform PIA / TRAs	<ul style="list-style-type: none"> ▪ LHINs should acquire appropriate expertise. ▪ Apply security considerations during all phases of the implementation lifecycle, (e.g. planning, procuring, Go-Live) ▪ Focus should be placed on the overall RM&R security strategy, as defined in the provided Security Framework, as opposed to focusing on specific requirements 	<ul style="list-style-type: none"> ▪ LHINs should approach other LHINs with RM&R implementations for expertise and recommendations.
Ensure that LHINs have a mature security program to support the RM&R solutions	<ul style="list-style-type: none"> ▪ Ensure adequate support and resources exist for a security program that can maintain and sustain the security requirements and practices required by the RM&R solution 	<ul style="list-style-type: none"> ▪ LHINs should assess their existing security program and provide required investment/support, where needed.
Ensure that vendor solutions under consideration are able to meet minimum security requirements	<ul style="list-style-type: none"> ▪ Ensure that vendors are aware of security requirements ▪ Ensure vendors have the ability to incorporate security requirements, as appropriate 	<ul style="list-style-type: none"> ▪ LHINs should ensure that potential RM&R solution vendors and/or design teams are aware of all security requirements prior to procurement discussions. ▪ Ensure security requirements are documented in contracts and Service Level Agreements and have an associated level of monitoring

Table of Contents

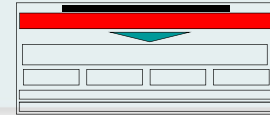
• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Security Background	Pages	13-16
– RM&R Security Framework	Page	13
– Security Guiding Principles	Page	14
– Key Assumptions	Page	15
– Opportunities and Recommendations	Page	16
• Security Requirements and Leading Practices	Pages	18-31
– Security Support for eReferral Process Enablement	Page	18
– Privacy Legislation and Security Requirements	Page	19
– RM&R Solution Security Requirements	Pages	20-25
– RM&R Operational Security Leading Practices	Pages	26-31
• Appendices	Pages	33-34
– Appendix 1: Security Requirements (Excel)	Page	33
– Appendix 2: Approach	Page	34

Support for eReferral Process Enablement

The Security Framework enables the eReferral process by ensuring that security requirements and leading practices are implemented as components of the overall RM&R solution.



Privacy Legislation and Security Requirements



The Ontario PHIPA speaks to privacy requirements for safeguarding PHI.

Privacy Legislation Requirements

Accountability

- The RM&R solution should have audit logging capabilities. (see section 6(3), 4. PHIPA, 2004 – O.Reg. 329/04)
- The Health Integration Network Provider (HINP) should provide Health Information Custodians (HICs) with a PIA and TRA for the RM&R solution. (see section 6(3), 5. PHIPA, 2004 – O.Reg. 329/04)

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)

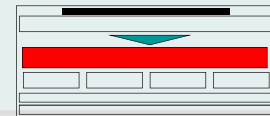
Collection of PHI

- The RM&R solution shall not acquire or disclose PHI from or to other external sources other than the HICs who are part of the RM&R solution. (see section 6(1), 2. PHIPA, 2004 – O.Reg. 329/04)

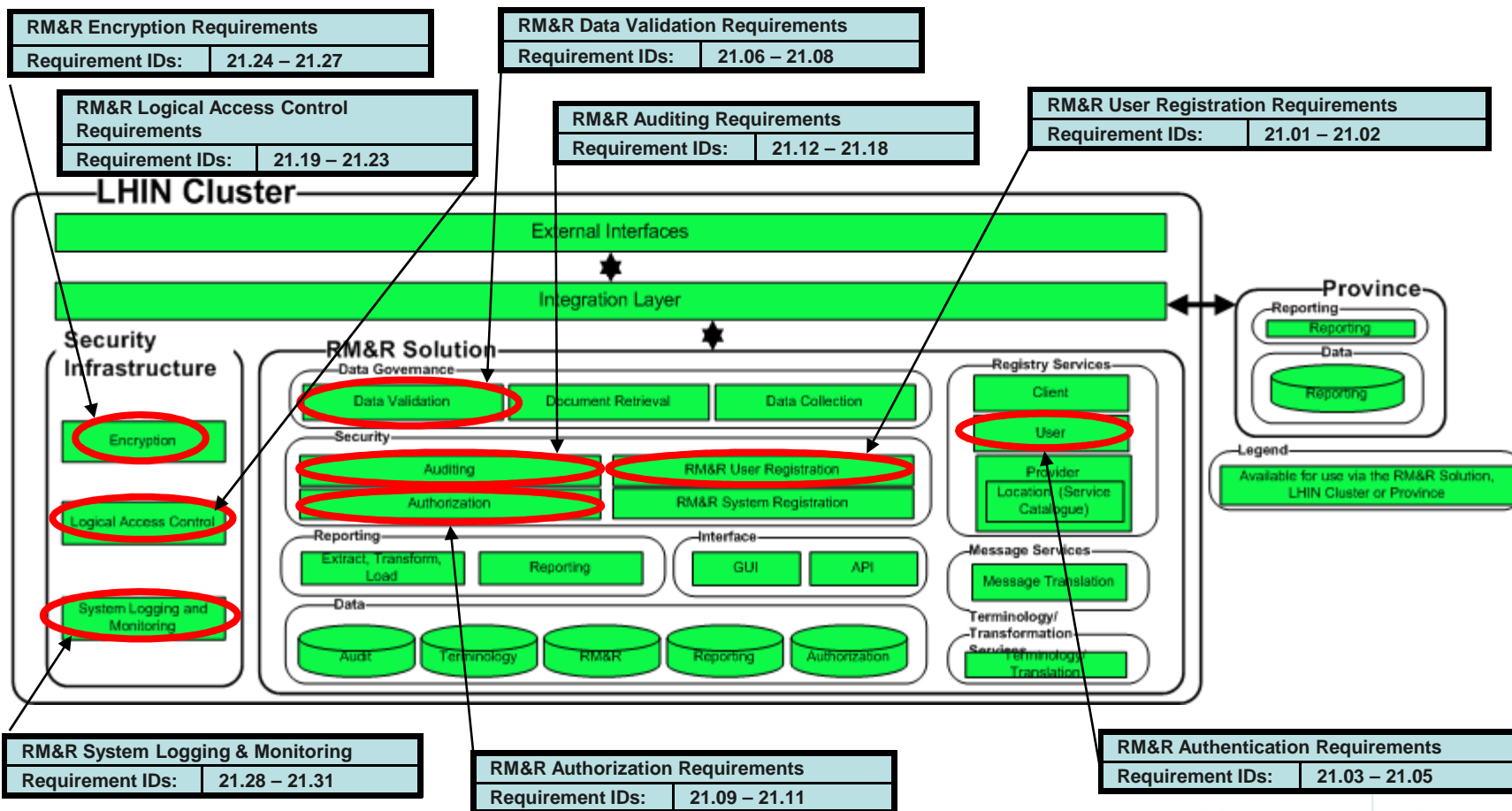
Consent

- The RM&R solution should support the following consent requirements:
 - Ability to record consent for the referral
 - Ability to record consent to send PHI to a referral destination
 - Ability to withdraw either type of consent
 - Ability to limit access to PHI from a particular user (see section 19(1) and 19(2). PHIPA, 2004)

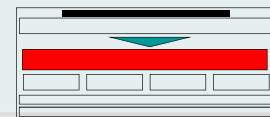
RM&R Solution Security Requirements (1 of 6)



The conceptual architecture diagram below provides context for the highlighted security requirement categories that should be considered for procurement purposes. The corresponding individual security requirements follow on the subsequent pages.



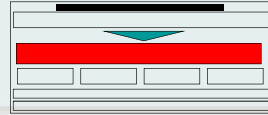
RM&R Solution Security Requirements (2 of 6)



This page and the following four pages provide a list of security requirements that should be considered when implementing a RM&R solution.

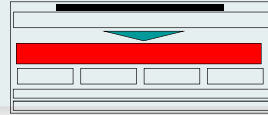
Number	Category	Description	Recommendation
21.01	User Registration	RM&R solutions should support a secure identity assurance process for user enrollment and credentials (e.g. password) resets. It should also implement a secure channel for credentials (e.g. password, token) distribution. Automated challenge response mechanisms when used should be assessed to ensure questions and responses cannot be easily guessed.	<ul style="list-style-type: none"> • Highly Recommended
21.02	User Registration	RM&R solutions should support distributed and hierarchical enrolment and administration of users to allow participating organizations (Health Information Custodians) to enroll and manage users.	<ul style="list-style-type: none"> • Nice to have
21.03	Authentication	The RM&R solution authentication services should ensure unique User IDs, complex passwords and/or two-factor authentication (e.g. tokens). Password policies should be configurable, granular and it should follow leading practices. (See NIST standards for more information on password strength).	<ul style="list-style-type: none"> • Highly Recommended
21.04	Authentication	For internet access consider risk-based authentication to grant access based on an evaluation of a wide range of parameters such as IP address and location. It may include challenge response or out-of-band (telephone) mechanisms to augment password based authentication.	<ul style="list-style-type: none"> • Highly Recommended
21.05	Authentication	RM&R solution should leverage existing robust Identity and Access Management solutions for registration, authorization and authentication services, whenever available. For example, implementing a single sign on solution or integrating with existing local clinical management systems authentication services. See Technology Solution framework for recommended authentication and authorization standard.	<ul style="list-style-type: none"> • Highly Recommended

RM&R Solution Security Requirements (3 of 6)



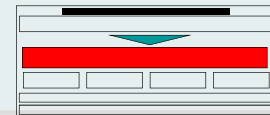
Number	Category	Description	Recommendation
21.06	Data Validation	RM&R solutions should validate messages against a defined schema. Messages containing invalid parameters should be rejected (e.g. reject text when expecting numeric).	<ul style="list-style-type: none"> • Highly Recommended
21.07	Data Validation	RM&R Solutions should protect against web vulnerabilities such as structured query language (SQL) script injection, parameter manipulation through the use of standard industry libraries to perform data validation. For example, use libraries provided by Java 2 Platforms, Enterprise Edition (J2EE), .NET frameworks and OWASP.	<ul style="list-style-type: none"> • Nice to have
21.08	Data Validation	LHINs or LHIN clusters should consider defining and enforcing strict data validation rules as part of business requirements and use cases.	<ul style="list-style-type: none"> • Highly Recommended
21.09	Authorization	RM&R solutions should authenticate and authorize each incoming request.	<ul style="list-style-type: none"> • Highly Recommended
21.10	Authorization	RM&R solutions should support an authorization model that is rule-based and takes into account multiple session parameters such as user-role, incoming channel, (e.g. internet, intranet, managed network) and time of request. This requirement is redundant if using a risk-based authentication model.	<ul style="list-style-type: none"> • Nice to have
21.11	Authorization	RM&R solutions should allow participating organizations (Health Information Custodian) to define specific access rules. LHIN or LHIN clusters should consider opportunities to investigate or create working groups to define common authorization policies.	<ul style="list-style-type: none"> • Nice to have

RM&R Solution Security Requirements (4 of 6)



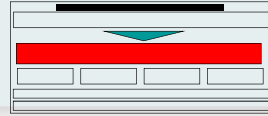
Number	Category	Description	Recommendation
21.12	Auditing	<p>RM&R solutions should capture and log the following event types:</p> <ul style="list-style-type: none"> • User activities, including viewing, updating and deleting patient records (i.e. PHI) • Critical processing errors (exceptions) • Failed access attempts (e.g. authentication and authorization failures) • Invalid Inputs 	• Highly Recommended
21.13	Auditing	RM&R solutions should restrict the amount of PHI data in a log when capturing user activities that access patient records.	• Highly Recommended
21.14	Auditing	<p>RM&R solutions should capture the following information when logging user activities:</p> <ul style="list-style-type: none"> • Who • When • Activity performed • Patient record accessed (when applicable) 	• Highly Recommended
21.15	Auditing	RM&R solutions should store logging information in a centralized location.	• Nice to have
21.16	Auditing	RM&R solutions should ensure that access to logs is restricted to authorized users only. Logs should be protected against inadvertent or deliberate changes to ensure integrity.	• Highly Recommended
21.17	Auditing	<p>RM&R solutions should provide the following auditing and reporting capabilities:</p> <ul style="list-style-type: none"> • List of current users and associated profiles • Users who have access to a specific patient record • Patient records that were accessed by a specific user • Inactive or dormant user accounts 	• Highly Recommended
21.18	Auditing	<p>RM&R solutions should be able to monitor and detect potential unauthorized access attempts and inappropriate use (as in financial fraud detection systems). These include:</p> <ul style="list-style-type: none"> • Ability to identify attempts to guess passwords • Potential abnormal behaviours, such as above average usage and off-hours access • Access from physically disperse, suspicious or unauthorized locations 	• Highly Recommended

RM&R Solution Security Requirements (5 of 6)



Number	Category	Description	Recommendation
21.19	Logical Access Control	<p>The RM&R solution should implement a layered architecture into security zones. Suggested security zones are:</p> <ul style="list-style-type: none"> • Demilitarized zone (DMZ) – front-end zone where all external connections should be terminated and authenticated (e.g. Secure Sockets Layer (SSL) Proxy, Extensible Markup Language (XML) Gateway) • Application zone – a zone hosting application servers where business logic is executed • Database zone – a zone that hosts database servers • Admin zone – remote system administration and infrastructure support (e.g. backup, system authentication, network monitoring) 	<ul style="list-style-type: none"> • Highly Recommended
21.20	Logical Access Control	All intra-zone (i.e. between security zones) communications should have flow control enforced through a firewall or equivalent level of network access policy enforcement.	<ul style="list-style-type: none"> • Highly Recommended
21.21	Logical Access Control	The RM&R solution should consider a centralized authentication service (e.g. RADIUS, directory services) for network devices and operating systems that can consistently enforce password and authentication standards.	<ul style="list-style-type: none"> • Nice to have
21.22	Logical Access Control	System administrators (e.g. Database Administrator (DBA)) connecting remotely should be authenticated to a high-level of assurance (i.e. using two-factor authentication).	<ul style="list-style-type: none"> • Highly Recommended
21.23	Logical Access Control	All system administrators' remote connections should terminate at a centralized Terminal Server in the Admin Zone. Only terminal emulation protocols, such as Remote Desktop Protocol (RDP) and Secure Shell (SSH) should be allowed (e.g. no direct connection from system administrator's remote desktops/laptops to systems should be allowed).	<ul style="list-style-type: none"> • Nice to have
21.24	Encryption	RM&R solutions should ensure all communications over uncontrolled networks (i.e. outside the boundaries of a secure data centre) are encrypted using an industry standard secure transport mechanism (e.g. SSL).	<ul style="list-style-type: none"> • Highly Recommended

RM&R Solution Security Requirements (6 of 6)

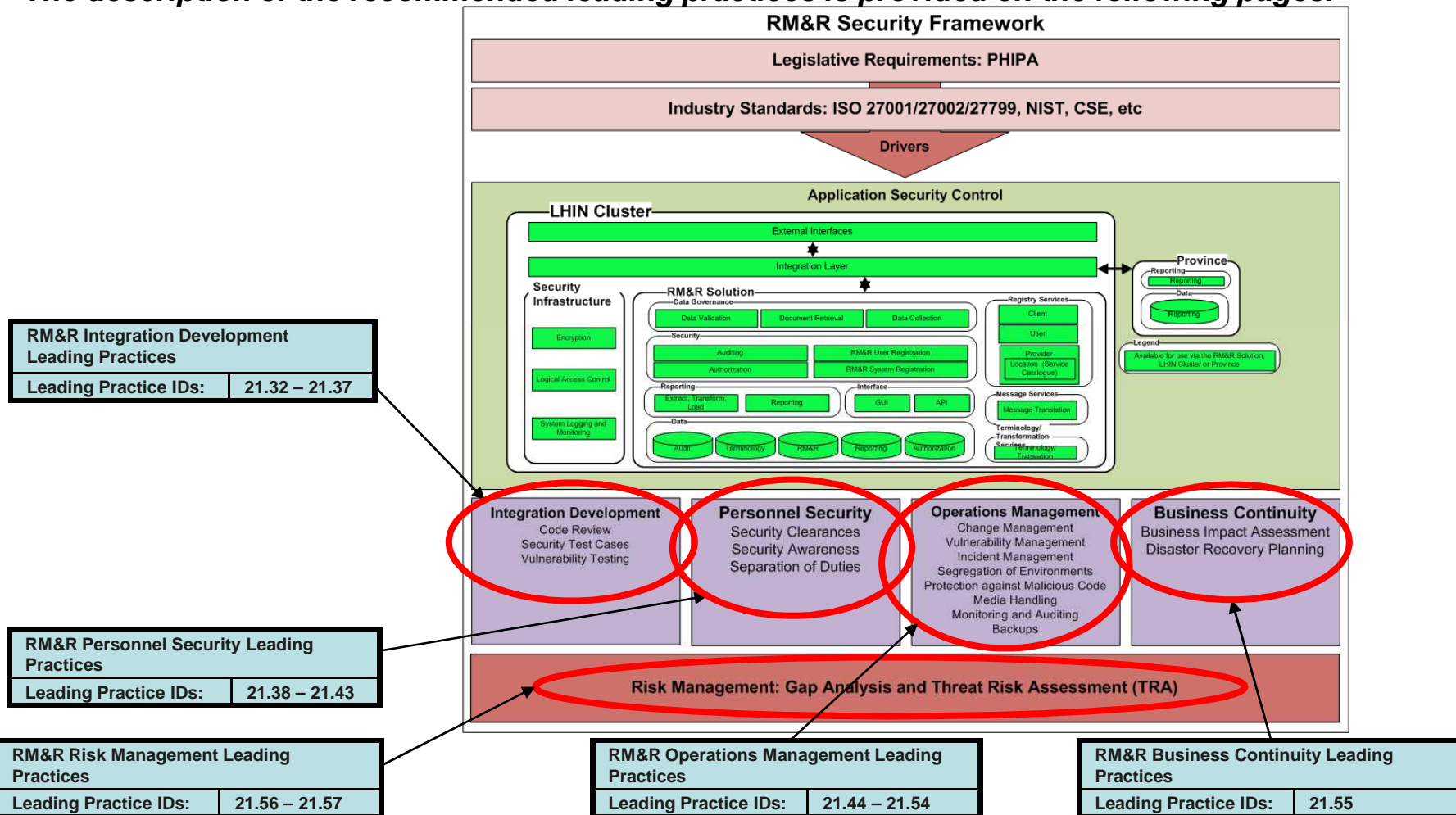


Number	Category	Description	Recommendation
21.25	Encryption	RM&R solutions should employ encryption algorithms implementations that are FIPS 140 compliant, preferably ones that have been certified (e.g. FIPS 140-2).	• Highly Recommended
21.26	Encryption	RM&R management processes should be designed and applied to ensure that encryption keys of cryptographic algorithms used in the RM&R solution are protected from unauthorized access and can be recovered in case of disasters. Cryptographic keys should be updated regularly in accordance with cryptographic module specifications to prevent cryptanalysis.	• Highly Recommended
21.27	Encryption	RM&R solutions should ensure that PHI information that is stored for long-term usage or that is to be removed off-site should be encrypted or have an equivalent level of physical security protection (e.g. highly secure data centre, escorted by trusted party).	• Highly Recommended
21.28	System Logging and Monitoring	RM&R solutions should ensure all communications originating from uncontrolled networks (i.e. outside the boundaries of a secure data centre) are monitored using Network Intrusion Detection/Prevention Systems (NIDS/NIPS).	• Highly Recommended
21.29	System Logging and Monitoring	RM&R solutions should consider a log management infrastructure, such as a Security Incident Management / Security Incident Event Management (SIM/SIEM) system to support the centralized storage, management, automated analysis and monitoring of system logs.	• Nice to have
21.30	System Logging and Monitoring	System administrator activities (e.g. login, configuration changes) should be logged to ensure proper accountability.	• Highly Recommended
21.31	System Logging and Monitoring	RM&R solutions systems should be adequately protected against malicious software.	• Highly Recommended

RM&R Operational Security Leading Practices (1 of 6)



The framework below provides leading operational security practices for operating a RM&R solution. The description of the recommended leading practices is provided on the following pages.



RM&R Integration Development Leading Practices
 Leading Practice IDs: 21.32 – 21.37

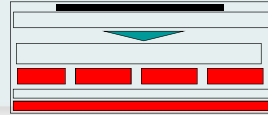
RM&R Personnel Security Leading Practices
 Leading Practice IDs: 21.38 – 21.43

RM&R Risk Management Leading Practices
 Leading Practice IDs: 21.56 – 21.57

RM&R Operations Management Leading Practices
 Leading Practice IDs: 21.44 – 21.54

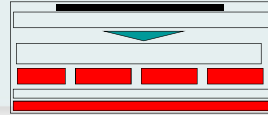
RM&R Business Continuity Leading Practices
 Leading Practice IDs: 21.55

RM&R Operational Security Leading Practices (2 of 6)



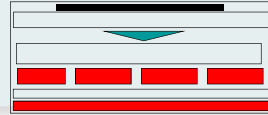
Number	Category	Description	Recommendation
21.32	Integration Development - Code Review	During RM&R solution development, any custom code should be reviewed in order to minimize the risk of software vulnerabilities (e.g. SQL injection, buffer overflow) and ensure coding best practices.	<ul style="list-style-type: none"> • Highly Recommended
21.33	Integration Development - Code Review	During RM&R solution development, static analysis of code by development teams should be considered using an automated tool before promoting code to production builds.	<ul style="list-style-type: none"> • Nice to have
21.34	Integration Development - Security Test Cases	<p>The RM&R Implementation team should develop and perform security test cases to demonstrate the implementation of application security requirements. Acceptance criteria should be defined and suitable security tests should be carried out prior to acceptance to production. These test cases should, at a minimum demonstrate that:</p> <ul style="list-style-type: none"> • Invalid and malicious input parameters are detected and logged • Invalid requests (malformed or that violates defined business rules) are being detected and logged • All logging requirements are being met • Alternative paths in use cases are tested 	<ul style="list-style-type: none"> • Highly Recommended
21.35	Integration Development – Vulnerability Testing	The RM&R Implementation team should ensure that vulnerability testing (e.g. grey box testing) by an independent party is conducted to identify software vulnerabilities. Specifically, web application vulnerability to attacks, such as cross-site scripting, SQL injection, parameter manipulation should be tested.	<ul style="list-style-type: none"> • Highly Recommended
21.36	Integration Development - Vulnerability Testing	During RM&R operations, major changes to application components or infrastructure should be followed up with vulnerability testing as these changes may have introduced additional vulnerabilities. Any change to application code should undergo security test case regression testing.	<ul style="list-style-type: none"> • Highly Recommended
21.37	Integration Development - Vulnerability Testing	During RM&R operations, vulnerability testing should be conducted periodically to maintain adequate security levels, as new security threats continue to emerge.	<ul style="list-style-type: none"> • Highly Recommended

RM&R Operational Security Leading Practices (3 of 6)



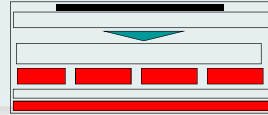
Number	Category	Description	Recommendation
21.38	Personnel Security - Security Clearance	LHINs should ensure that development and operations team members have security clearance appropriate to the level of responsibility for their role. Background checks should be performed that are commensurate with the sensitivity of their role and access to PHI.	<ul style="list-style-type: none"> Highly Recommended
21.39	Personnel Security - Security Awareness	LHINs should ensure that all members of the development and operations teams have the appropriate level of security and privacy training and demonstrated proficiency in said training to the level of responsibility of their role.	<ul style="list-style-type: none"> Highly Recommended
21.40	Personnel Security - Security Awareness	LHINs should ensure that all members of the development and operations teams are educated on privacy principles and requirements as per Ontario's Personal Health Information Protection Act (PHIPA), 2004.	<ul style="list-style-type: none"> Highly Recommended
21.41	Personnel Security - Security Awareness	LHINs should ensure that all members of the development and operations teams have their security role and responsibilities defined within their job description.	<ul style="list-style-type: none"> Nice to Have
21.42	Personnel Security - Security Awareness	LHINs should ensure that all members of the development and operations teams sign non-disclosure and acceptable use agreements.	<ul style="list-style-type: none"> Highly Recommended
21.43	Personnel Security - Separation of Duties	LHINs should ensure that duties and areas of responsibilities are segregated in order to reduce opportunities for unauthorized and unintentional modification or misuse of the system. For instance, the same person should not make system changes and have access to audit logs.	<ul style="list-style-type: none"> Nice to Have
21.44	Operations Management - Change Management	All updates and changes to RM&R solution systems should be properly tested, documented and managed, ensuring that only authorized individuals have access to key systems and code. A change management procedure should be documented to ensure strict change management controls.	<ul style="list-style-type: none"> Highly Recommended

RM&R Operational Security Leading Practices (4 of 6)



Number	Category	Description	Recommendation
21.45	Operations Management - Vulnerability Management	<p>The RM&R solution production environment should be hardened following industry best practices (e.g. US National Institute of Standards and Technology (NIST) or Government of Canada Communication Security Establishment guidelines). This should include:</p> <ul style="list-style-type: none"> • An up-to-date system inventory maintained to support the identification of system vulnerabilities • All operating systems and network devices systems scanned against known vulnerabilities at regular intervals • A patch management procedure defined to support the vulnerability management process 	<ul style="list-style-type: none"> • Highly Recommended
21.46	Operations Management - Incident Management	<p>The RM&R solution should be supported by a documented security incident management procedure to ensure security incidents and issues are identified, escalated, contained and resolved in a timely fashion.</p>	<ul style="list-style-type: none"> • Highly Recommended
21.47	Operations Management – Segregation of Environments	<p>The implementation of the RM&R solution should ensure that development, testing, and operational environments are segregated to reduce the risk of unauthorized access or changes to operational environments.</p>	<ul style="list-style-type: none"> • Highly Recommended
21.48	Operations Management - Segregation of Environments	<p>The implementation of the RM&R solution should ensure that no sensitive production data (e.g. PHI) is copied to test or development environments without being de-identified or properly masked. Exceptions should be documented and approved on the assumption the test environment has the same level of security as the production environment and that test users have the appropriate level of clearance to see the sensitive data (e.g. PHI).</p>	<ul style="list-style-type: none"> • Highly Recommended
21.49	Operations Management - Protection against Malicious Code	<p>The RM&R solution should provide a mechanism to automatically update malicious code signatures. In addition, a procedure should be documented for the manual recovery of systems infected with malicious code.</p>	<ul style="list-style-type: none"> • Highly Recommended

RM&R Operational Security Leading Practices (5 of 6)



Number	Category	Description	Recommendation
21.50	Operations Management - Media Handling	The RM&R solution should have documented procedures for the secure management of removable media. The use of removable media should be employed for business specific needs only.	• Highly Recommended
21.51	Operations Management - Media Handling	The RM&R solution should ensure that all media taken offsite that contains sensitive information such as PHI is encrypted. A log of media sent off-site should be recorded.	• Highly Recommended
21.52	Operations Management - Media Handling	The RM&R solution should have documented procedures in place for the secure disposal of media containing sensitive information. Physical and/or technical controls should be defined to ensure data cannot be recovered from decommissioned media or when there is a change of use.	• Highly Recommended
21.53	Operations Management - Monitoring and Auditing	The RM&R solution should ensure that logging, monitoring and auditing requirements are documented and consistent with open industry standards. This includes: <ul style="list-style-type: none"> • Robust error monitoring, reporting, logging and auditing functionality are required across all components of the solution • Granular authentication and authorization are supported to access audit log content • System clocks are synchronized from a centralized accurate time source 	• Highly Recommended
21.54	Operations Management - Backups	The RM&R solution should ensure that: <ul style="list-style-type: none"> • Backups are done in a manner and schedule that ensures there is no data loss in the event of a catastrophic failure of one or more system components • A backup strategy is implemented that supports availability requirements • Restore procedures are established that include the testing of backup tapes on regular basis 	• Highly Recommended
21.55	Business Continuity – Business Impact Assessment / Disaster Recovery Planning	The RM&R solution should ensure that a business continuity plan is created and documented. This includes a business impact assessment, disaster recovery planning and business recovery analysis. A review of existing business continuity and disaster recovery plans should be conducted to evaluate if they will meet the needs of the RM&R solution.	• Highly Recommended

RM&R Operational Security Leading Practices (6 of 6)



Number	Category	Description	Recommendation
21.56	Risk Management: Gap Analysis and TRA - Privacy Impact Assessments	The RM&R solution should be subjected to a PIA and any recommendations stemming from the PIA should be incorporated into the solution, where applicable. Residual risks should be signed off by senior management.	<ul style="list-style-type: none"> Highly Recommended
21.57	Risk Management: Gap Analysis and TRA - Threat/Risk Assessments	The RM&R solution should be subjected to a TRA and any recommendations stemming from the TRA should be incorporated into the solution, where applicable. Residual risks should be signed off by senior management	<ul style="list-style-type: none"> Highly Recommended

Table of Contents

• Context	Pages	3-8
• Executive Summary	Pages	10-11
• Security Background	Pages	13-16
– RM&R Security Framework	Page	13
– Security Guiding Principles	Page	14
– Key Assumptions	Page	15
– Opportunities and Recommendations	Page	16
• Security Requirements and Leading Practices	Pages	18-31
– Security Support for eReferral Process Enablement	Page	18
– Privacy Legislation and Security Requirements	Page	19
– RM&R Solution Security Requirements	Pages	20-25
– RM&R Operational Security Leading Practices	Pages	26-31
• Appendices	Pages	33-34
– Appendix 1: Security Requirements (Excel)	Page	33
– Appendix 2: Approach	Page	34

Appendix 1: Security Requirements

- Detailed Security Requirements are available as a separate attachment.

Requirements (PDF):

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

Appendix 2: Security Component Approach

- The ALC RM&R project team established a Business Process & Data Standards 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 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.
- Using the business process flows, conceptual architecture, privacy legislation and security leading practices & industry standards as input, the ALC RM&R security team developed a list of security requirements and operational leading practices that should be considered when planning and implementing security for a RM&R solution.