University Health Network (UHN)

RESOURCE MATCHING AND REFERRAL (RM&R) AND ONLINE REFERRAL BUSINESS INTELLIGENCE TOOL (ORBIT)

Policy Governing User Account Management

Version: 4.0
Date: Last modified on September 17, 2020

Table of Contents

1. User Registration Policy

This policy provides information on how to register users, including helpdesk users, and provide access to the Resource Matching and Referral (RM&R) application and/or the Online Referral Business Intelligence Tool (ORBIT). It includes the following information:

- Identifying and outlining the responsibilities of the *Registration Authority (RA)*
- Identifying and outlining the responsibilities of the *Helpdesk Administrator (HDA)*
- Identifying and outlining the responsibilities of the *Local Registration Authority (LRA)*
- Registration process for a *User*
- Registration process for, and responsibilities of, the *Helpdesk User (HDU)*
- Management of user accounts and the escalation framework

There is a clear distinction in this policy between *Users* and *Helpdesk Users (HDUs).* A *HDU* is a specific type of *User* having user management privileges. The HDU role allows Participating Organizations to self-manage RM&R user accounts (e.g., account creation or deactivation, password reset) without any assistance from the RM&R Support Desk, operated by Strata Health Solutions. Participating Organizations without a HDU would have their LRA authorize the creation or deactivation of a user account, and then the RM&R Support Desk would process the change request instead of the HDU.

1.1 Participating Organization's Policy for Access Control

The Participating Organization should develop a formally written *Access Control Policy* for regulating access to RM&R, and/or the HDU role. Alternatively, the organization's formally written *Information Security Policy* may be used in place of a separate access control policy; however, it must include the required details regarding the HDU role. In addition, all users, including HDUs, must be subjected to a formal registration process and ensure adherence to this policy.

Procedures must include and ensure:

a) An individual is designated as the LRA to register new users (i.e., authenticate and authorize the creation of user accounts), including HDUs.
b) The level of user identification provided is consistent with the eHealth Ontario's Assurance Level 2 (Medium Assurance Level) requirements, given the value of the information assets and functions available to the user.
c) Each potential user, including a HDU, is an Agent of the organization (as defined in PHIPA, 2004).
d) Each HDU will be providing RM&R user account management administrative support.
e) Conditions or limitations thereof pertaining to the appropriate use of user accounts, including the HDU role, are specifically outlined and consistent with the requirements of this policy, including the prevention of user account creation, the rights and responsibilities related to having access to Personal Health Information (PHI), and an explicit restriction for accessing PHI for any purposes other than supporting users in providing, or assisting, in the provision of health care to patients.

2. Roles and Responsibilities

2.1 Registration Authority (RA)

The RM&R Program will serve as the RA for each Participating Organization using the RM&R application and/or ORBIT.

The RA assumes the function of authorizing the creation or modification of LRA and HDU accounts, and acting upon received LRA or HDU Registration Forms that have been properly completed and sponsored by either the Participating Organization's Senior Management, or an existing LRA directly appointed by the Senior Management. The member of Senior Managemet must, at minimum, be an individual legally tied to the Participating Organization (e.g., Executive Director).

The **RA** is responsible for:

- governing the designation of LRAs, HDAs, and HDUs validating users according to eHealth Ontario's Assurance Level 2 (Medium Assurance Level) requirements;
- managing and maintaining the LRA, HDA, and HDU registry;
- maintaining the RM&R User Role Matrix;
- overseeing adherence to the registration and management processes identified in this document;
- overseeing adherence to the privacy and security policies of the RM&R Program;
- liaising with LRAs, HDAs, and HDUs on registration issues (see section 5 for the escalation framework); and,
- implementing authenticated requests for (the creation or modification of) user accounts, including user accounts for LRAs or HDUs, or delegating select authority to process these requests to the HDA.

2.2 Helpdesk Administration (HDA)

The HDA oversees the appropriate processing of user account creation and modification requests as per the LRA in absence of a local HDU. The RM&R Support Desk, which is operated by Strata Health Solutions, will serve as the HDA, and function in accordance with the RM&R and ORBIT Support Desk Guidelines. It is important to note that the RM&R Support Desk provides all levels of support to users, including the troubleshooting of referrals; however, the scope of this policy is applicable to agents providing only user account management support. In providing user account management support, the HDA only has permissions to access the administration module in the RM&R application, and will not have access to Patient Health Information (PHI) or referral-specific information.

The **HDA** is responsible for:

- ensuring appropriate privacy and security safeguards are followed, and in accordance with the RM&R and ORBIT Support Desk Guidelines;
- creating or modifying user accounts (e.g., account reactivation, password resets, role assignment changes, changes to unit/service provider access) following receipt of documented and/or properly authorized requests from an organization's LRA, or Senior Management;

- confirming that only persons meeting the criteria of providing or assisting in the provision of healthcare are granted access to RM&R or ORBIT, including those granted with HDU status, and excluding researchers;
- liaising with the RA, LRAs, and HDUs on registration issues, as prescribed by the RA (see section 5 for the escalation framework);
- serving as a single point of contact for the RA, LRAs, HDUs, and Users;
- communication to LRAs, HDUs, and users of new policies and procedures, as prescribed by the RA; and,
- updating training documents and training a HDU before the HDU can provision any RM&R user accounts.

2.3 Local Registration Authority (LRA)

LRAs are appointed or designated by 'trusted individuals' within their organization. These 'trusted individuals' can include either the organization's Senior Management, or, an existing LRA directly appointed by a member of the Senior Management.

There are two types of LRAs: LRAs sponsored by their organization's Senior Management are classified as **Appointed LRAs**. LRAs sponsored by their organization's Appointed LRA are classified as **Designated LRAs**, and may perform all duties of an Appointed LRA except designating additional LRAs.

LRAs ensure the secure and appropriate registration of the organization's users requiring access to the RM&R or ORBIT applications, including HDUs or additional LRAs, by authenticating and subsequently authorizing each user request. Essentially, LRAs are responsible for managing user accounts, including the level of access and user account modifications, at their organization. This ensures that each site, in accordance with the security and privacy policies of their organization and of the RM&R Program, will securely manage user accounts.

The LRA is a role assumed by individuals who have been delegated by their organization to perform user account management duties. Each Participating Organization must identify both a primary (Appointed) LRA and a secondary (Appointed or Designated) LRA. In the event that the primary LRA becomes unavailable on short notice, the secondary LRA will assume responsibilities, ensuring full coverage at all times for the organization.

The **LRA** is responsible for:

- identifying your organization's RM&R and ORBIT users, including HDUs and Privacy Officers;
- adhering to the *Access Control Policy* for RM&R and ORBIT, and identity management processes within your organization for all users;
- adhering to processes and procedures as prescribed by this policy;
- validating users according to eHealth Ontario's Assurance Level 2 (Medium Assurance Level) requirements;
- advising the HDA or HDU as soon as a user at your organization no longer requires access, either by communicating the fact directly or by inference in setting up or terminating an account;

- advising the RA as soon as he/she can no longer maintain the duties of a LRA and/or is leaving the organization so a suitable replacement can be established in a timely manner, if necessary;
- adhering to privacy and security policies and procedures within the organization, and of the RM&R Program;
- validating and authenticating individuals requesting a user account , or HDU status, confirming that they are eligible to access the RM&R and/or ORBIT applications (or have HDU status) by consulting with your organization's Privacy Officer (PO), your organization's PO-equivalent, or the RA;
- validating that only persons meeting the criteria of providing or assisting in the provision of healthcare are granted access to RM&R or ORBIT, including those granted with HDU status, and excluding researchers;
- managing, documenting, and tracking user account management requests;
- reviewing user access on a quarterly basis and removing or modifying access, as appropriate;
- reporting privacy incidents to your organization's Privacy Office;
- participating in privacy investigations, as required;
- validating, authenticating, and subsequently authorizing changes to user accounts;
- answering questions pertaining to a user's authorized permissions;
- answering questions pertaining to the validation, authentication, or authorization of user accounts; and,
- liaising with the RA, HDAs, and HDUs on user registration issues (see section 5 for the escalation framework).

The LRA's authorization is required by the HDA or HDU when change requests are made for the following:

1. Addition of a new user account, including the addition of bulk user accounts. LRAs must use the RM&R User Management Template to complete these requests – the RA (RMR_Program@uhn.ca) may be contacted to obtain a copy of this template.
2. Deactivating, or activating a user account that was previously deactivated.
3. Modification to user account and/or access, including:
    - Change in the role and/or function assigned to the user as defined by the RM&R User Role Matrix and RM&R policies.
    - Change in the service providers/units the user may access.
    - Change in the user's assigned Remote ID (Integration ID).
    - Change in user's name.

Users may directly contact the HDA or HDU for resetting their password or activating an expired account. Any change requests to add, remove, or modify roles or service providers/units associated with a Participating Organization cannot be authorized by the LRA; however, they may still provide the requirements for the change to the HDA, and the appropriate business approval (e.g., RM&R User Group member).

The following is a high-level outline of the process:

Step	Description
1	The 'trusted individual' at the Participating Organization determines which individual(s) will be assigned the role of LRA.
2	The Participating Organization completes the LRA Registration Form, identifying the LRA accordingly. The LRA form is signed by the Participating Organization's 'trusted individual.'
3	The Participating Organization submits the completed form to the RA.
4	The Participating Organization provides the LRA with training on performing the roles and responsibilities of a LRA, as well as, this policy.
5	The RA updates the LRA Registry accordingly.

Only the RA has the authority to change the status of the LRA on behalf of a Participating Organization. These changes include granting, suspending, and revoking the LRA appointment. To ensure full coverage of the LRA responsibilities, LRAs must inform the RA when leaving (and will no longer be employed by) a Participating Organization. The RA will liaise with the Participating Organization or remaining Appointed LRA to establish a replacement in a timely manner.

When the RA **grants** an individual LRA status, he/she is executing the Participating Organization's intent to authorize the individual to collect, verify, and submit registration requests for new RM&R or ORBIT users (i.e., authenticating and authorizing the creation, modification, or deactivation of user accounts) on behalf of the organization.

When the RA **suspends** a LRA, he/she is temporarily removing the LRAs authority to collect, verify, and submit registration requests for new RM&R or ORBIT users (i.e., authenticating and authorizing the creation, modification, or deactivation of user accounts) on behalf of the organization. Possible reasons for LRA suspension include, but are not limited to, extended leaves, such as maternity leave or sabbatical.

When the RA **revokes** an individual's LRA status, he/she is removing the LRAs authority to collect, verify, and submit registration requests for new RM&R or ORBIT users (i.e., authenticating and authorizing the creation, modification, or deactivation of user accounts) on behalf of the organization. If the individual subsequently needs to become a LRA, the request must be re-submitted. Possible reasons for LRA revocation include, but are not limited to: an individual no longer wishes to perform the role of LRA; an individual is no longer associated with the Participating Organization; or an individual's inability to perform the LRA duties.

2.4 Helpdesk User (HDU)

HDUs are appointed or designated by 'trusted individuals' within their organization. This 'trusted individual' can include a member of Senior Management, or an existing HDU directly appointed by the Senior Management.

There are two types of HDUs: HDUs sponsored by their organization's Senior Management are classified as **Appointed HDUs**. HDUs sponsored by their organization's Appointed HDU are classified as **Designated HDUs**, and may perform all duties of an appointed HDU except designating additional HDUs.

The HDU ensures the secure and appropriate registration of individuals requiring access to the RM&R application at an organization as per this policy and the LRA's authorization. The HDU is not permitted to access Personal Health Information (PHI), and therefore, the creation of HDU accounts having access to PHI is strictly prohibited.

The **HDU** is responsible for:

- adhering to the registration and/or identity management processes within their organization;
- adhering to processes and procedures as prescribed by this policy;
- adhering to privacy and security policies and procedures within the organization, and of the RM&R Program;
- reporting privacy incidents to the Participating Organization's Privacy Office;
- ensures the secure and appropriate registration of individuals requiring access to RM&R at an organization;
- liaising with and obtaining authorization from the LRA, or Senior Management, prior to performing account management activities (see section 5 for the escalation framework);
- ensuring account changes are well-documented in the Identity Log, and that documentation can be made available upon request;
- adhering to policies and procedures for non-expiring accounts, as applicable; and,
- receiving and completing full training from the HDA before provisioning any RM&R user accounts

Each Participating Organization has the choice of opting into this program, identifying HDUs and/or changing the status of existing HDUs.

The following is a high-level outline of the process:

Step	Description
1	The 'trusted individual' at the Participating Organization determines which individual(s) will be assigned the role of HDU.
2	The Participating Organization completes the HDU Registration Form, identifying the HDU accordingly. The HDU Enrolment Form is signed by the Participating Organization's 'trusted individual.'
3	The Participating Organization submits the completed form to the RA.
4	The HDA provides training to the HDU before the HDU can provision any RM&R user accounts. The HDU is trained on performing the roles and responsibilities of a HDU, this policy document, and

	relevant RM&R privacy and security policies and procedures. The HDA will document all correspondence with the HDUs during the registration period and report this to the RA.
5	The RA updates the HDU Registry accordingly.

Only the RA has the authority to change the status of the HDU on behalf of a Participating Organization. These changes include granting, suspending, and revoking the HDU appointment.

When the RA **grants** HDU status to an individual, the RA is executing the Participating Organization's intent to authorize the individual to collect, verify, and complete account change requests (i.e., create, modify, or deactivate accounts) for their RM&R users.

When the RA **suspends** HDU status from an individual, the RA is temporarily removing the HDUs authority to collect, verify, and complete account change requests (i.e., create, modify, or deactivate accounts) for RM&R users. Possible reasons for HDU suspension include, but are not limited to, extended leaves, such as maternity leave, sabbatical, or privacy/security investigations.

When the RA **revokes** HDU status from an individual, the RA is removing the HDUs authority to collect, verify, and complete account change requests (i.e., create, modify, or deactivate accounts) for RM&R users. If the individual subsequently needs to become a HDU, the request must be re-submitted. Possible reasons for HDU revocation include, but are not limited to; an individual no longer wishes to perform the role of HDU; an individual is no longer associated with the Participating Organization; or an individual's inability to perform the HDU duties.

3. Management of User Accounts

3.1 Registration or Modification of User Accounts

Any user wishing to access RM&R or ORBIT is required to contact their LRA for approval. It is the responsibility of the LRA to ensure that they have verified the user's identity according to eHealth Ontario's Assurance Level 2 (Medium Assurance Level) requirements before they submit the new user request to either the HDA or the HDU, depending upon their organization's set up.

3.2 User Password Resets

There is a strict procedure to be followed when users require their passwords to be reset. Users must submit requests to reset their password directly to the HDA or HDU. For security reasons, the HDA or HDU must only provide temporary passwords to users directly, requiring users to reset their passwords upon login.

Users must adhere to the minimum password requirements as prescribed in the RM&R Privacy and Security HIC Manual. It is important to note that password resets are only applicable to Participating Organizations accessing the application(s) through a non-integrated environment (please see Appendix A for definition).

3.3 Handling Departing Users and Internal Controls

The LRA, on behalf of their Participating Organization, must promptly notify the HDA or HDU to terminate the access privileges of a user upon termination of their employment, contract, or other relationship with the Participating Organization. The HDA or HDU is required to deactivate the user's account immediately and within one business day, at latest. For organizations having a HDU, the HDU must also log this change in the Identity Log.

Access to RM&R or ORBIT should be reviewed on a quarterly basis and user accounts should be deactivated or modified as appropriate by the LRA. In addition, a record of audits and changes should be maintained. The Participating Organization should develop and implement a policy and procedure for terminating access privileges.

3.4 Maintaining an Identity Log

The Participating Organization must require that the LRA and/or HDU maintain a log to track all activities performed, inclusive of all changes to RM&R or ORBIT user accounts. Please see below for an example of an Identity Log.

Figure 3-1: Identity Log Example

First Name	Last Name	PathWays Username (Email Address)	Role	Site	Account Change	Date	Account Status
John	Doe	John.Doe@ABCHospital.ca	Appointed LRA	ABC Hospital	Create account	1/1/2015	Active
Jane	Doe	Jane.Doe@ABCHospital.ca	Designated LRA	ABC Hospital	Suspend account	1/1/2015	Deactivated
Jack	Roe	Jack.Roe@ABCHospital.ca	Appointed HDU	ABC Hospital	Create account	1/1/2015	Active
Ava	Bouvet	Ava.Bouvet@ABCHospital.ca	Designated HDU	ABC Hospital	Revoke account	1/1/2015	Deactivated
Luca	Mancini	Luca.Mancini@ABCHospital.ca	Privacy Officer	ABC Hospital	Departing User	6/15/2015	Deactivated
Owen	Smith	Owen.Smith@ABCHospital.ca	Physician	ABC Hospital	Activate account	7/15/2015	Active
Jane	Roe	Jane.Roe@ABCHospital.ca	RN	ABC Hospital	Create account	8/15/2015	Active

4. Account Expiration

RM&R user accounts are set to expire after 120 days of account inactivity by default. Should a user's RM&R account expire due to inactivity, the user may contact their Local Service Desk, HDU, LRA, and/or HDA for reactivation.

ORBIT user accounts do not expire due to inactivity. The account remains active until the RM&R Program receives notification to deactivate the user account.

4.1 RM&R Non-Expiring Accounts

Participating Organizations operating within an integrated environment may opt in to have all their RM&R user accounts set to never expire; non-integrated environments do not have this option at this time. Selecting this option will ensure that all RM&R user accounts created for that Participating Organization will never expire due to inactivity. However, as a result of this decision, the Participating Organization's LRA will assume all responsibility and liability for managing and maintaining RM&R user accounts for that Participating Organization. This includes performing periodic audits of user accounts for validation purposes, and ensuring to properly request the disabling of accounts upon the departure of users. In order to select this option, the Participating Organization's Senior Management must complete and submit the RM&R Service Enrolment Form.

In opting to have non-expiring user accounts, the Participating Organization is required to meet or exceed account management requirements as specified in the RM&R Privacy and Security HIC Manual**.** The RM&R Account Management Exception Form is to be used by a Participating Organization to request exemption from a mandatory requirement. Once the site's requester has completed Section 1 of the form, the requester must send the form to RMR_Program@uhn.ca. Each exception request will be sent to the RM&R Privacy and Security Team for processing.

5. Escalation Framework

Any issues regarding the registration process established within this document should be reported and escalated based on the following hierarchy:

> ***Users*** should report issues by escalating to their respective *Helpdesk User (HDU)* or *Local Registration Authority (LRA).*
>
> ***Helpdesk Users (HDU)*** should report issues by escalating to their respective *Local Registration Authority (LRA)* or *Helpdesk Administrator (HDA)*.
>
> The ***Local Registration Authority (LRA)*** should report issues by escalating to the *Helpdesk Administrator (HDA)* or *Registration Authority (RA)*.
>
> The ***Registration Authority (RA)*** can be contacted via email at RMR_Program@uhn.ca, which is the RM&R Program.
>
> The ***Helpdesk Administrator (HDA)*** can be contacted via email at referrals@uhn.ca, which is the RM&R Support Desk.

APPENDIX A: Glossary of Terms

HDA – Help Desk Administrator; responsible for managing HDU accounts

HDU – Help Desk User; responsible for creating/modifying user accounts within an organization, as per the authorization of the site's LRA

Integrated Environment – referring to a Participating Organization that accesses the Resource Matching & Referral (RM&R) application via that organization's Hospital Information System (HIS), by way of a single sign-on protocol

Local Registration Authority – an individual designated by the Participating Organization to manage the Resource Matching and Referral (RM&R) User Registration process on behalf of said organization

LRA – see *Local Registration Authority*

Participating Organization – a site that is participating in the usage of the RM&R application

RA – see *Registration Authority*

Resource Matching and Referral – the Resource Matching and Referral application, or RM&R

Registration Authority – the entity that governs the User registration process and policy, or RA

RM&R – see *Resource Matching and Referral*

User – a user of (the RM&R) application (e.g., clinician)

APPENDIX B: LRA Registration Form

RM&R and ORBIT Local Registration Authority (LRA) Registration Form

Form Completion Instructions

1. Complete all fields as specified. Mandatory fields are marked with an asterisk (*). If the form is incomplete, it will be returned to you. Indicate "Not Applicable" or "N/A" if the field is not applicable.
2. Part 2 of the form must be completed by either:
    i. your organization's Senior Management in order to sponsor an Appointed LRA; or
    ii. your organization's existing and previously authorized Appointed LRA (sponsored by your organization's Senior Management) in order to sponsor a Designated LRA. Designated LRAs cannot sponsor additional LRAs.
3. Please e-mail a scanned copy of the original form signed and completed to: rmr_program@uhn.ca
4. If you have any questions regarding the completion of this form or the RM&R and ORBIT LRA registration process, please email the RM&R Program at rmr_program@uhn.ca.

Part 1 – RM&R/ORBIT Local Registration Authority Applicant Details

Applicant Details - *This section is to be completed by the **applicant**. The applicant is the individual who is applying to become a RM&R/ORBIT Local Registration Authority for your organization.*

Legal First Name *	Job Title *	Legal Last Name *
Business Telephone *(include ext.)* * ( )	Business Fax ( )	Business Email *

Site/Hospital Name *(e.g., ABC General Hospital, ABC Community Health Centre)* *

Business Address *(Number and Street)* *	Suite/Unit/Floor	City/Town *	Prov * **ON**	Postal Code *

Change Request Details *

☐ *Grant Authority*	☐ *Revoke Authority*	☐ *Suspend Authority*
Grant the LRA's authority to collect, verify, and submit registration requests for RM&R or ORBIT users.	Permanently remove the LRA's authority to collect, verify, and submit registration requests for RM&R or ORBIT users.	Temporarily remove the LRA's authority to collect, verify, and submit registration requests for RM&R or ORBIT users.

Reason (specify):

I confirm that I will adhere to all tenets of the RM&R and ORBIT Policy Governing User Account Management.

Applicant's Signature * Date Signed *(yyyy-mm-dd)* *

Part 2 – Sponsor Details

Sponsor Details - *This section is to be completed by your organization's **Senior Management**, or an existing and previously authorized **Appointed Local Registration Authority**. Specify your organization's name and address only if different from the applicant; however, contact information (e.g., business telephone and/or business email) must be provided. Please note that an existing and previously authorized Designated Local Registration Authority cannot act as a sponsor.*

Legal First Name *	Middle Initial(s)	Legal Last Name *
Title *(e.g., CEO, CIO)* *	Business Telephone *(include ext.)* * ( )	Business Email *

Site/Hospital Name *(e.g., ABC General Hospital, ABC Community Health Centre)* *

Business Address *(Number and Street)* *		Suite/Unit/Floor	
City/Town *	Province * **ON**	Postal Code *	Date of Request *(yyyy-mm-dd)* *

I confirm that I have reviewed the applicant's identity documents and this application for registration.

Sponsor's Signature * Date Signed *(yyyy-mm-dd)* *

☐ ***I authorize the appointment and/or change of status of the Local Registration Authority above.*** *

Print Form

APPENDIX C: HDU Registration Form

RM&R Help Desk User (HDU) Registration Form

Form Completion Instructions

1. Complete all fields as specified. Mandatory fields are marked with an asterisk (*). If the form is incomplete, it will be returned to you. Indicate "Not Applicable" or "N/A" if the field is not applicable.
2. Part 2 of the form must be completed by either:
    i. your organization's Senior Management; or
    ii. your organization's existing and previously authorized (Appointed or Designated) LRA.
3. Please e-mail a scanned copy of the original form signed and completed to: rmr_program@uhn.ca
4. If you have any questions regarding the completion of this form or the HDU registration process, please email the RM&R Program at rmr_program@uhn.ca.

Part 1 – RM&R Helpdesk User (HDU) Applicant Details

Applicant Details - *This section to be completed by the **applicant**. The applicant is the individual who is applying to become a RM&R Helpdesk User for your organization.*

Legal First Name *	Job Title *	Legal Last Name *
Business Telephone *(include ext.)* * ( )	Business Fax ( )	Business Email *

Site/Hospital Name *(e.g., ABC General Hospital, ABC Community Health Centre)* *

Business Address *(Number and Street)* *	Suite/Unit/Floor	City/Town *	Prov *	Postal Code *
			ON	

Change Request Details *

☐ *Grant Authority*	☐ *Revoke Authority*	☐ *Suspend Authority*
Grant the HDU's authority to collect, verify, and complete account change requests for RM&R users.	Permanently remove the HDU's authority to collect, verify, and complete account change requests for RM&R users.	Temporarily remove the HDU's authority to collect, verify, and complete account change requests for RM&R users.

Reason (specify):

I confirm that I will adhere to all tenets of the RM&R and ORBIT Policy Governing User Account Management.

Applicant's Signature * Date Signed *(yyyy-mm-dd)* *

Part 2 – Sponsor Details

Sponsor Details - *This section is to be completed by your organization's **Senior Management**, or an existing and previously authorized (Appointed or Designated) **Local Registration Authority**. Specify your organization's name and address only if different from the applicant; however, contact information (e.g., business telephone and/or business email) must be provided.*

Legal First Name *	Middle Initial(s)	Legal Last Name *
Title *(e.g., CEO, CIO)* *	Business Telephone *(include ext.)* * ( )	Business Email *

Site/Hospital Name *(e.g., ABC General Hospital, ABC Community Health Centre)* *

Business Address *(Number and Street)* *		Suite/Unit/Floor	
City/Town *	Province * **ON**	Postal Code *	Date of Request *(yyyy-mm-dd)* *

I confirm that I have reviewed the applicant's identity documents and this application for registration.

Sponsor's Signature * Date Signed *(yyyy-mm-dd)* *

☐ ***I authorize the appointment and/or change of status of the Help Desk User above.*** *

APPENDIX D: Service Enrolment Form

RM&R Service Enrolment Form

Form Completion Instructions

1. Complete all fields as specified. Mandatory fields are marked with an asterisk (*). If the form is incomplete, it will be returned to you. Indicate “Not Applicable” or “N/A” if the field is not applicable.
2. The form must be completed by your organization’s Senior Management.
3. Please e-mail a scanned copy of the original form signed and completed to: rmr_program@uhn.ca
4. If you have any questions regarding the completion of this form or the RM&R service enrolment process, please email the RM&R Program team at rmr_program@uhn.ca.

Part 1 - Organization-Level RM&R Account Expiry Exemption

Expiry Exemption *- This section is to be completed by the* ***Senior Management (i.e. Executive Director, Administrator, CIO or CEO)****.*

Site/Hospital Name *(e.g., ABC General Hospital, ABC Community Health Centre)* *			
Business Address *(Number and Street)* *		Suite/Unit/Floor	
City/Town *	Province * **ON**	Postal Code *	Date of Request *(yyyy-mm-dd)* *
Change Request Details *			
☐ *Opt for Non-Expiring Accounts* Opt to have all the RM&R accounts associated with this site/hospital exempted from the default account expiration. All current and future accounts created for this site/hospital will never expire due to inactivity: they will have to be manually deactivated when required.		☐ *Opt for Expiring Accounts* Opt to have all the RM&R accounts associated with this site/hospital be rendered expired should the account be inactive for a period of 120 days. All current and future accounts created for this site/hospital will be affected by this change.	

Part 2 – Signing Authority Details

Signing Authority Details - *This section is to be completed by the* ***Senior Management****.*

Legal First Name *	Middle Initial(s)	Legal Last Name *	
Title *(e.g., CEO, CIO)* *	Business Telephone *(include ext.)* * ( )	Business Email *	
Site/Hospital Name *(e.g., ABC General Hospital, ABC Community Health Centre)* *			
Business Address *(Number and Street)* *		Suite/Unit/Floor	
City/Town *	Province * **ON**	Postal Code *	Date of Request *(yyyy-mm-dd)* *
Signing Authority's Signature *		Date Signed *(yyyy-mm-dd)* *	