Operations User Guide

Hospital Report Manager

Version: 1.5

Document Control

The electronic version of this document is recognized as the only valid version.

Document Location: www.ontariomd.ca/ir/hrmdocs

Approval History

Approver(s)	Title	Approved Date
Brian Forster	Chief Executive Officer	2013-09-26

Revision History

Version No.	Date	Summary of Change	Changed By
0.1	2013-04-08	Initial draft	Gosia Kacprzak
0.2	2013-04-29	Content revisions	Gosia Kacprzak
0.3	2013-05-02	Content edits and additions	Lawrence Chan
0.4	2013-05-16	Content and style edits	Communications HRM Privacy Physician IT Services Product Management
0.5	2013-05-21	Formatting updates	Gosia Kacprzak
0.6	2013-05-21	Style updates	Communications
0.7	2013-06-19	Content and style edits	Brian Forster
0.8	2013-07-11	Content and style edits	Gosia Kacprzak
0.9	2013-07-16	Internal stakeholder feedback updates	Gosia Kacprzak
1.0	2013-07-23	Content edits and additions	Lawrence Chan
1.1	2013-08-12	Content edits to reflect pPIA recommendations	Gosia Kacprzak Communications
1.2	2013-09-11	Content and style edits	Brian Forster
1.3	2013-09-17	Content and style edits	Brian Forster
1.4	2013-09-26	Final Review	Brian Forster
1.5	2013-12-10	Privacy Updates, Formatting	Gosia Kacprzak

Table of Contents

1. About This Document

1.1 Purpose and Scope

The purpose of this document is to present the concepts and support processes related to Hospital Report Manager (HRM) operations. It is intended for hospital and Independent Health Facility (IHF) Health Care Providers and staff in Ontario that currently send text-based reports via HRM to primary care practices and for physician or nurse practitioner-led practices using a Funding Eligible EMR offering that complies with EMR Specification 4.1a or greater to receive text-based reports via HRM.

1.2 Reference Material

The following documents, available on the OntarioMD website www.ontariomd.ca/ir/hrmdocs, were referenced for the development of this Operations Guide:

- HRM Subscriber OntarioMD Service Level Agreement
- HRM Privacy Policy
- HRM Privacy Breach Management Policy
- OntarioMD Privacy Complaints and Inquiry Policy and Procedures
- Privacy & Encryption Online Tutorial

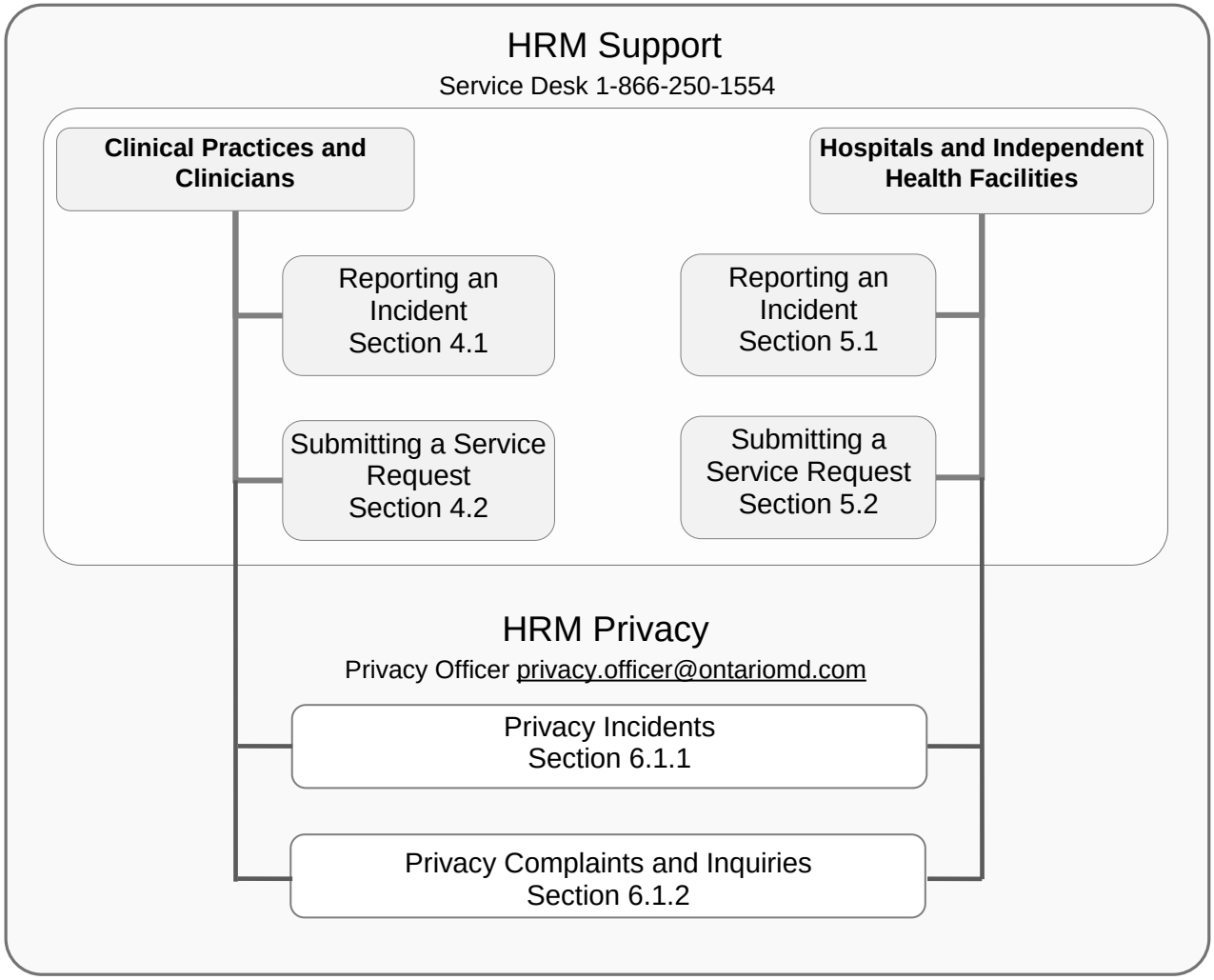
2. Support Overview

2.1 HRM Support

The eHealth Ontario Service Desk is the central point of contact for support for the Hospital Report Manager (HRM) provincial solution. To ensure the eHealth Ontario Service Desk can process your request as quickly as possible, please follow the steps below.

2.2 HRM Privacy

For privacy related incidents contact the OntarioMD Privacy Officer directly at: privacy.officer@ontariomd.com. The eHealth Ontario Service Desk should ***not*** be contacted for reporting privacy related incidents.



3. HRM Application Overview

The Hospital Report Manager (HRM) enables hospitals to electronically transmit patient reports to practice-based physician's Electronic Medical Record (EMR). This solution replaces the existing process of paper copies and faxes being sent to the physician's office and either manually entered into the EMR or managed outside of the EMR. With the introduction of the HRM, hospital reports are updated directly to the patient's electronic medical record for a physician to access in a timely and less labour intensive manner.

For additional information about the HRM please visit www.ontariomd.com/hrm.

4. Support Processes for Clinical Practices and Clinicians

If you are experiencing a problem with HRM, follow the steps in section 4.1 to resolve issue. If you need to make changes that affect your HRM service or profile information, contact the Service Desk by submitting a service request as outlined in section 4.2.

4.1 Reporting an Incident

Examples of Incidents	Category
• I have not received a report that I am expecting • I cannot open/view my report • I have received a duplicate report(s) • My report cannot be downloaded by the EMR • I received a report that is not intended for me • My report contains incorrect PHI	**Error/ Issue Encountered**

Before reporting an incident:

1. Verify that your EMR is connected to HRM.
2. Have your internal IT support or EMR vendor check that your systems are functioning properly.
3. If you are missing a report, contact the hospital/independent health facility to ensure the report was sent.
4. Prepare the following information to provide to eHealth Ontario's Service Desk personnel:
   - First and last name
   - CPSO/CNO number
   - Clinic address
   - Contact information

HRM support process:

5. Call the Service Desk at 1-866-250-1554 and specify that your incident is related to HRM.
6. Specify the issue that you are experiencing.
   - Identify the steps that you took to confirm that this is an HRM issue.
   - Provide as much information as you can about the issue, including details about the specific report (e.g. report number), if available.
7. Service Desk personnel will open a ticket and provide you with a ticket number. Keep this number for your reference in the event that follow-up is required.
8. eHealth Ontario Service Desk will work with OntarioMD, as required, to identify the cause of the issue.
   - If additional information is required, you may be contacted by a HRM representative from OntarioMD.
   - OntarioMD will also contact the relevant report sender, if required.
9. Once your incident has been resolved, the Service Desk will contact you to close the ticket.

4.2 Submitting a Service Request

Examples of Service Request s	Category
• I would like to edit my HRM profile (e.g. name, CPSO, etc.) or my clinic's HRM profile (e.g. address, contact information, etc.) • I would like to be added to or removed from HRM	**Operational Request**
• My EMR will undergo network changes (e.g. firewall, IP addresses, ports, etc.) • I am changing hardware in my practice (e.g. servers, routers and other devices, etc.) • I am updating or changing my EMR software	**System Maintenance**
• I would like to receive an audit log about my recent HRM activity • I would like to know who has had access to my PHI	**Reporting Request**

If there are any changes to your system, profile information or clinic information, please inform the Service Desk as soon as possible to ensure that your reports are delivered in a timely manner. It is particularly important to inform the Service Desk if you are leaving a practice to ensure Personal Health Information (PHI) is redirected appropriately.

Before submitting a request:

1. Make sure that you have all the relevant information about your request and that your information is accurate.
2. Prepare the following information to provide to eHealth Ontario's Service Desk personnel:
   - First and last name
   - CPSO/CNO number
   - Clinic address
   - Contact information

HRM support process:

3. Call the Service Desk at 1-866-250-1554 and specify that your service request is related to HRM.
4. Specify the nature of your request.
   - Provide as much information as you can about your request, including the date that the change will be effective.
5. Service Desk personnel will open a ticket and provide you with a ticket number. Keep this number for your reference in the event that follow-up is required.
   - If additional information is required, you may be contacted by a HRM representative from OntarioMD.
6. Once your request has been fulfilled, the Service Desk will contact you to close the ticket.

5. Support Processes for Hospitals and Independent Health Facilities

If you are experiencing a problem with HRM, follow the steps in section 5.1 to resolve the issue. If you need to make changes that affect your HRM service or profile information, contact the Service Desk by submitting a service request as outlined in section 5.2.

5.1 Reporting an Incident

Examples of Incidents	Category
• A report was sent to the wrong recipient • Duplicate report(s) were sent to a recipient • A production report (with PHI) was sent to the development environment • A development report (without PHI) was sent to the production environment • Several reports are queued up and are not going through	**Error/Issue Encountered**

Before reporting an incident:

1. Verify that your site is connected to HRM.
2. Have your internal IT support check that your systems are functioning properly.
3. Be prepared to provide the following information to eHealth Ontario's Service Desk personnel:
   - First and last name
   - Facility name
   - Site name and address (if facility has multiple sites)
   - Contact information

HRM support process:

4. Call the Service Desk at 1-866-250-1554 and specify that your incident is related to HRM.
5. Specify the issue that you are experiencing.
   - Identify the steps that you took to confirm that this is an HRM issue.
   - Provide as much information as you can about the issue, including details about the specific report, if relevant.
6. Service Desk personnel will open a ticket and provide you with a ticket number. Keep this number for your reference in the event that follow-up is required.
7. eHealth Ontario Service Desk will work with OntarioMD, as required, to identify the cause of the issue.
   - If additional information is required, you may be contacted by a HRM representative from OntarioMD.
   - OntarioMD will also contact the relevant report recipient, if required.
8. Once your incident has been resolved, the Service Desk will contact you to close the ticket.

5.2 Submitting a Service Request

Examples of Service Requests	Category
• I would like to edit my facility's HRM profile (e.g. name, address, contact information, etc.) • I would like to add/ edit/ delete a report type	**Operational Request**
• The facility's information system will undergo network changes (e.g. firewall, IP addresses, ports, etc.) • The facility is changing hardware (e.g. servers, routers and other devices, etc.) • My facility is updating software (e.g. HIS, OS, ADT, Interface Engine, etc.)	**System Maintenance**
• I would like to receive an audit log about my facility's HRM activity • I would like to know who has had access to my facility's PHI	**Reporting Request**

If there are any changes to your system, profile information or facility information, inform the Service Desk as soon as possible to ensure that your reports are delivered in a timely manner. It is particularly important to inform the Service Desk if you expect downtime of your internal system(s).

Before submitting a request:

1. Make sure that you have all the relevant information about your request and that your information is accurate.
2. Prepare the following information to provide to eHealth Ontario's Service Desk personnel:
   - First and last name
   - Facility name
   - Site name and address (if the facility has multiple sites)
   - Contact information

HRM support process:

2. Call the Service Desk at 1-866-250-1554 and specify that your service request is related to HRM.
3. Specify the nature of your request.
   - Provide as much information as you can about your request, including the date that the change will be effective.
4. Service Desk personnel will open a ticket and provide you with a ticket number. Keep this number for your reference in the event that follow-up is required.
   - If additional information is required, you may be contacted by a HRM representative from OntarioMD.
5. Once your request has been fulfilled, the Service Desk will contact you to close the ticket.

6. Privacy

NEVER share Personal Health Information (PHI)

To ensure PHI data remains secure, do not discuss PHI on the phone and do not send unencrypted emails with PHI in them.

As custodians of PHI, Health Care Providers (HCP) have obligations under the *Personal Health Information Protection Act*, 2004 (PHIPA) and Ontario Regulation 329/04 (the "Regulation"). It is the responsibility of each HCP to ensure that in collecting, using, retaining and disclosing PHI related to the HRM, it is in compliance with its obligations under:

1. All agreements entered into between OntarioMD and the HCP or the organization for which the HCP works (whether as an employee, partner, agent, or under contract) to ensure compliance with applicable privacy legislation, policies and procedures.
2. PHIPA and Ontario Regulation 329/04 (the "Regulation")
3. Any other applicable legislation or regulation, and
4. Any applicable judicial or administrative tribunal judgments, orders, rulings, or decisions.

The HCP is responsible for obtaining the consent of the patient to collect, use, retain or disclose PHI.

For additional information about the roles and responsibilities of a HCP and PHIPA, please visit the OntarioMD website for a Privacy & Encryption Online Tutorial.

For the purposes of the Hospital Report Manager (HRM), OntarioMD acts as a Health Information Network Provider (HINP) as regulated by section 6 of O. Reg. 329/04 to the *Personal Health Information Protection Act* (PHIPA). In accordance with PHIPA, the safeguarding of an individual's privacy is critical to OntarioMD's role as a HINP for the HRM application.

A HINP is defined as, "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians;" Ontario Reg. 329/04, s. 6 (2). This section 6 of O. Reg. 329/04 to PHIPA requires OntarioMD to notify every applicable Health Information Custodian (HIC) at the first reasonable opportunity if, in the course of providing services to enable a HIC to use electronic means to collect, use, disclose, retain or dispose of PHI, the PHI has been stolen, lost or accessed by unauthorized persons.

6.1 Privacy Procedures

The procedures below outline, at a high level, the requirements for handling a privacy breach and submitting a complaint or inquiry. For more detailed information relating to HRM Privacy Policy and Breach Management Procedures, please visit www.ontariomd.ca/ir/hrmdocs.

6.1.1 Privacy Incidents

A privacy incident includes the collection, use or disclosure of Personal Information (PI) or PHI that is not in compliance with applicable privacy laws, or circumstances where PI or PHI is stolen, lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.

Authorized HRM users, including report sending HICs such as hospitals, and receiving HICs such as physician offices, who are made aware of a suspected or confirmed privacy incident related to the HRM are instructed to follow their internal privacy policies and procedures as well as report the incident to the OntarioMD Privacy Officer (Privacy Officer). Patient notification of the privacy incident should be handled by the HIC through their internal incident reporting processes.

Before reporting a HRM related privacy incident:

1. Follow your internal privacy policies/procedures to notify the appropriate parties of the privacy incident.

Reporting a HRM related privacy incident:

2. Contact the Privacy Officer to notify OntarioMD of the suspected/actual privacy incident:
   - By email: privacy.officer@ontariomd.com
   - By phone: 416-340-2900
3. Describe the suspected or actual privacy incident.
   - Do ***not*** include PHI in the description of the privacy incident.
3. OntarioMD will determine if the incident originated in HRM.
   - If so, OntarioMD will work to immediately contain or support the containment of all reported privacy incidents to prevent further unauthorized collection, use and/or disclosure of PI or PHI.
5. Once a privacy breach has been effectively contained, it will be investigated and the details of the incident and investigation will be documented.
   - The documentation will include the recommendations emanating from the investigation with timeframes for the recommendations to be implemented.
6. The Privacy Officer will maintain a log of privacy breaches and the recommendations emanating from investigations of these breaches.

When acting under the capacity of a HINP, OntarioMD will notify HICs if it identifies that a privacy breach has occurred. When required, as determined by the Privacy Officer, OntarioMD will notify the Information and Privacy Commissioner of Ontario of the incident, investigation and remediation plan.

6.1.2 Privacy Complaints and Inquiries

Individuals can obtain information about OntarioMD's privacy policies and procedures on OntarioMD's website. Individuals may submit a complaint or inquiry relating to OntarioMD's privacy policies, procedures and guidelines by contacting the OntarioMD Privacy Officer.

Submitting a privacy complaint or inquiry:

1. Submit your complaint or inquiry to the Privacy Officer via one of the following methods:
   - By email: privacy.officer@ontariomd.com
   - By phone: 416-340-2900
   - By mail: OntarioMD Inc.
     150 Bloor Street West
     Suite 900
     Toronto, Ontario, M5S 3C1, Canada
     Attention: OntarioMD Privacy Officer
2. When making a complaint or inquiry, include the following information:
   - A detailed description of the complaint or inquiry
   - Date and time of an occurrence
   - Individuals involved in an occurrence
   - Any other pertinent information
3. The Privacy Officer acknowledges receipt of a complaint or inquiry within five (5) business days of receiving the complaint or inquiry. All privacy complaints and inquiries are reviewed by the Privacy Officer.
   - Where the sender has provided their contact information, OntarioMD may contact the individual to clarify the nature or scope of the complaint or inquiry.
4. The Privacy Officer is responsible for assessing the complaint or inquiry and determines whether or not to proceed with an investigation.
   - The decision is sent in a letter to the complainant within ten (10) business days of the receipt of the complaint or inquiry.
5. Within twenty (20) business days of the receipt of the complaint or inquiry, the Privacy Officer completes the investigation and documents the findings from the interviews, reviews and site visits in a report.

If OntarioMD is contacted with a complaint or inquiry regarding a HIC's information management or privacy practices, it will direct the individual to the appropriate HIC. If a complaint about a HIC could have an impact on OntarioMD's contract management and compliance monitoring activities, OntarioMD may choose to follow up with the HIC regarding the investigation and resolution.

7. Appendix A – Glossary

Term	Description
Health Information Custodian (HIC)	A health information custodian is defined under section 3 of the *Personal Health Information Protection Act, 2004* (PHIPA) as a: • Health care practitioner, as an individual, or as part of a group practice (e.g. a physician, dentist, nurse, social worker; any person whose primary function is to provide health care for payment) • Person or organization that provides a community health service • Community Care Access Centre • Public or private hospital • Psychiatric facility • Long-term care facility • Pharmacy • Laboratory or specimen collection centre • Ambulance service • Board of Health • Ministry of Health and Long-Term Care **NOTE:** For the purposes of HRM, eHealth Ontario is not a HIC. HICs must comply with PHIPA and are responsible for the management and safeguarding of personal health information.
Health Information Network Provider (HINP)	A HINP is defined as, "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians." O. Reg. 329/04, s. 6 (2).
Personal Health Information (PHI)	Section 2 of the *Freedom of Information and Protection of Privacy Act* (FIPPA) defines PHI as "recorded information about an identifiable individual", including: (a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual (b) Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved (c) Any identifying number, symbol or other particular assigned to the individual (d) The address, telephone number, fingerprints or blood type of the

Term	Description
	individual (e) The personal opinions or views of the individual except where they relate to another individual (f) Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence (g) The views or opinions of another individual about the individual, and The individual's name where it appears with other Personal Information (PI) relating to the individual or where the disclosure of the name would reveal other PI about the individual.
Personal Information (PI)	As defined in section 2 of the *Freedom of Information and Protection of Privacy Act* (FIPPA), "recorded information about an identifiable individual, including, (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, telephone number, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they relate to another individual, (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, and (h) the individual's name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual."
Privacy Incident	A privacy incident includes the collection, use or disclosure of Personal Information (PI) or Personal Health Information (PHI) that is not in compliance with applicable privacy laws, or circumstances where PI or PHI is stolen, lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.