OntarioMD

HOSPITAL REPORT MANAGER SUBSCRIBER - ONTARIOMD SERVICE LEVEL AGREEMENT

CONTENTS

SECTION 1 EXECUTIVE SUMMARY

1.1 Overview

The Ontario Hospital Report Manager (HRM) is an automated solution for the electronic transmission of hospital reports typically between the local hospital report contributor systems and Clinicians' Electronic Medical Record (EMR) systems. This document is a Service Level Agreement (SLA) between a Hospital Report Manager (HRM) Subscriber and OntarioMD, the manager of the HRM.

A Subscriber is defined as a Health Information Custodian (HIC) that originates and sends electronic patient reports to HRM. A HIC can be an organization and/or an end user that is identified as the recipient of the patient reports.

1.2 Purpose

The purpose of this agreement is to:

A. Provide HRM subscribers with an understanding of HRM services – what is included and what is excluded;
B. Describe the support services available and how to contact/initiate support when required; and
C. Set service level expectations.

1.3 HRM Support Contact

HRM Support Contact covers two support services:

A. Incident Management; and
B. HRM Service Requests.

A. Incident Management

The eHealth Ontario Service Desk is the **single point of contact** with end users for incident management for the Hospital Report Manager application. The eHealth Ontario Service Desk is responsible for receiving incident calls from the end users and engaging either the OntarioMD Service Desk or eHealth Ontario's Technical Operations Centre.

Support Business Hours:	24 hours a day / 7 days a week / 365 days a year
Service Phone Number:	1.866.250.1554
Service Email:	servicedesk@ehealthontario.on.ca

**Note: The primary contact method for end users to report incidents to the eHealth Ontario Service Desk is by telephone. There is currently no SLA for incidents opened by the eHealth Ontario Service Desk via email.*

B. HRM Service Requests

The eHealth Ontario Service Desk is the **single point of contact** for service requests related to:

A. Clinician enrollment and de-enrollment to receive reports from hospitals;
B. Information requests regarding report types provided by a hospital; and
C. Ad-hoc transactional/audit report requests.

Support Business Hours:	24 hours a day / 7 days a week / 365 days a year
Service Phone Number:	1.866.250.1554
Service Email:	servicedesk@ehealthontario.on.ca

**Note: The primary contact method for end users to open service requests with the eHealth Ontario Service Desk is by telephone. There is currently no SLA for service requests opened by the eHealth Ontario Service Desk via email.*

Regulative Environment, Service Conditions & Constraints

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

Regulative Environment - Information Privacy & Security

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 personal health information (PHI), the PHI has been stolen, lost or accessed by unauthorized persons.
Authorized HRM end users, including contributing HICs such as hospitals, and consuming HICs such as clinical practices, who are made aware of a confirmed or suspected privacy or security breach related to the HRM, are instructed to follow their internal breach management policies and procedures as well as to report the breach to OntarioMD's Privacy Officer. For additional information about OntarioMD's Privacy Policy please visit: www.ontariomd.ca.

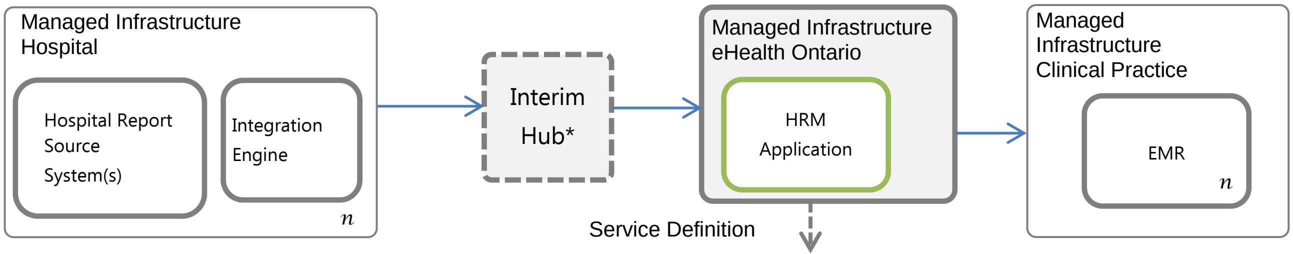
Appropriate and authorized access to PHI by the parties is described in detail in the Subscription Services Agreement.

The two core services provided by HRM are:

1. Transformation of content in hospital reports into a standard message format that can be used by EMRs meeting OntarioMD EMR Specifications 4.1 or higher; and

2. Brokerage and delivery of the report to a secure area for pick-up by an EMR.

The following is a service definition breakdown and is intended to provide a framework for the services provided.



2.1 Service Operations

2.1.1 HRM receives report	2.1.2 The report is transformed from the hospital's report standard to an EMR native format.	2.1.3 Report is routed to the clinical practice's designated secure folder.	2.1.4 HRM facilitates clinical practice's EMR to retrieve report.

2.1.5 Service Underpinnings

A – Transactional Reporting Services	B – Report Type Awareness	C – Security, Privacy and Connectivity

2.2 Service Requests

2.2.1 Clinician Enrollment / De-Enrollment to receive reports from a hospital.	2.2.2 Information requests regarding report types provided by a hospital	2.2.3 Ad hoc Transactional / Audit report.

2.3 Service Exclusions

2.3.1 Identity and Access Management for hospital or clinic IT systems.	2.3.2 Report handling services including redirection, re-sending, re-formatting.	2.3.3 Report content augmentation, deletion or edits.	2.3.4 Deletion of report within HRM secure folder. (EMR responsibility)	2.3.5 Data management services - responsibilities, conditions and limitations	2.3.6 Deployment services including EMR configuration and EMR related technical support.

3 IT Service Management (ITSM) – Service Operations Processes

3.1 Service Request Fulfillment	3.2 Incident Management – Tier 2 Support	3.4 Change Management including: 1) HRM application maintenance; 2) Emergency change (bug fixes); 3) HRM deployment to new hospitals; 4) HRM application enhancements; and 5) HRM application changes due to EMR specification maturity.	3.5 Business Continuity
	3.3 Problem Management – Tier 3 Support		3.6 Service Restoration

Table 1: HRM Service Overview

* *Refer to Schedule D for details of transmission via a hub.*

2.1 Service Operations

Overall Service Preconditions

A. Hospital is a registered HRM facility and the HRM Deployment Package has been successfully deployed and the secure folder established;

B. Receiving clinician has / is:

   I. A CPSO/CNO number;

   II. A registered user for the selected hospital’s report source systems;

   III. The required access rights and permissions for all interrelated IT systems managed within the hospital or clinic; and

C. Clinician practice uses an EMR that conforms to OntarioMD EMR Specification 4.1 or higher and the clinic’s EMR has been configured to utilize the HRM service.

2.1.1 HRM receives report.

Service Preconditions	A. The report is filed using the hospital’s report source systems; B. The Integration Engine managed by the hospital identifies the report recipients and prepares the report for sending to HRM; and C. The Integration Engine sends the report to HRM. This is a push service, i.e., the request for a given transmission is initiated by the hospital report source systems.
Service Provisions	Upon receipt of the report, HRM validates that the report has been received in its entirety and sends an acknowledgement to the HRM Integration Engine. A success or fail of the report transmission will be reported to the hospital’s HRM Integration Engine: A. On success, no further action is required; or B. On failure, the hospital will correct and resend report. If issues remain, contact Incident Management Support Services. C. The transaction is logged for audit purposes
Service Limitations	A. No report content is validated, augmented or deleted. B. OntarioMD will inform the hospital when HRM receives a report for delivery to a clinician who is not enrolled to HRM. C. HRM will disregard and purge data elements not required for HRM, as per deployment specifications.

2.1.2 The Report is transformed from the hospital's report standard to an EMR native format.

Service Preconditions	A. The report has been successfully received by the HRM from the hospital.
Service Provisions	A. HRM transforms the report from the hospital's standard to the EMR Specification standard.
Service Limitations	A. No report content is validated, augmented or deleted.

2.1.3 Report is routed to the clinician practice's designated secure folder.

Service Preconditions	A. The clinician practice's designated secure folder has been successfully created and is operational
Service Provisions	A. HRM utilizes a User Registry to map the identified recipient(s) to the clinic's secure folder. Upon identification of the clinician practice, the report is encrypted using the file encryption key associated with the EMR instance for the clinic. The report is then stored within the identified clinician practice's secure folder. Processing Time Frame – The report will be processed and delivered to the relevant clinician practice secure folder no more than 30 minutes from the time the report is received from Integration Engine from where it will be available for the clinicians EMR to retrieve the report. B. The transaction is logged for audit purposes.

2.1.4 HRM facilitates clinic's EMR to retrieve report.

Service Preconditions	A. HRM will use a secure connection with appropriate controls, to allow the EMR to retrieve the report from the clinic's designated secure folder. The transaction is logged for audit purposes.
Service Provisions	A. Clinic's EMR Responsibilities: I. Retrieve the report from HRM. This is a pull service, i.e., the request for a given transmission is initiated by the clinic's EMR. The timing is determined by the EMR's configuration as per the Specification or can be initiated ad hoc as per the configuration implemented. Note: The availability of the report for retrieval is contingent on the hospital's submission to HRM. II. The EMR will delete the report from the secure folder. III. The EMR will decrypt the report using the file decryption key. IV. The EMR will manage the delivery and storage of the report to the receiving clinician. B. HRM Responsibilities I. OMD continually monitors the SFTP folders to ensure timely retrieval by the clinic EMRs. If a report is not retrieved by the clinic's EMR within 24 hours of delivery to their designated secure folder, HRM Notification Services will send an alert to OntarioMD's HRM Support Team and to the clinic. The HRM Support Team will contact the clinic to notify it that a report is awaiting pick-up and will provide troubleshooting support, as appropriate, until the issue has been resolved. OntarioMD will continue to work directly with the clinic, and respective hospital, as appropriate, to ensure successful resolution of the issue. If a report cannot be picked up by the clinic's EMR after issue resolution, the sending hospital may be asked to re-send the report, to the affected recipient, via HRM or other means. II. If a clinic does not download a HRM (MR/DI text-based) report from the SFTP folder and is not responsive as part of the operational process outlined above, OntarioMD will notify the report sender 5 days before the files will be purged. Reports will be purged if they have not been picked up by the clinic's EMR within 28 days of being placed in the clinic's designated secure folder. OntarioMD will contact and notify the clinic that reports are waiting to be retrieved. Any reports that have remained in a clinic's designated secure folder for longer than 28 days will be purged after notifying the clinic that the reports have not been picked up.

2.1.5 Service Underpinnings

The following services provide operational support and are available by design through the HRM system or based on HRM requirements.

A. Transactional Reporting Services

Transactional reports are available for monitoring and auditing HRM system functionality. Please contact eHealth Ontario's Support Desk for more information on these services.

B. Report Types Awareness

Over time, new report types become available within a hospital. It is critical for the timely announcement of new report types and to configure EMR's to receive the new report types to ensure the flow of reports via HRM are not interrupted.

Responsibilities	**Details**
I. **Hospital**	• The hospital is to inform via the eHealth Ontario Support Contact of a new report type and its definition within a reasonable timeframe to ensure the flow of reports to clinician practice's EMR.
II. **OntarioMD**	• OntarioMD will provide report types and its definition to HRM subscribers to ensure EMR's are configured to receive the new reports; and • OntarioMD will make available the list of report types for hospitals for awareness and reference by clinician practitioners utilizing an EMR.
III. **Clinician Practice EMR IT Support Services**	• Ensure new report types are added and configured for the clinician practitioner's EMR.

C. Security, Privacy & Connectivity

I. **Maintain Security Certificates**	A. OntarioMD will maintain the required security certificates and make available the security certificates' status upon request.
II. **Data Integrity and Data Encryption**	A. HRM services will be deployed as per Specification.
III. **EMR Specifications**	A. EMR secure access to HRM, data encryption and the file retrieval process are managed in accordance with the connectivity requirements defined in the current EMR Specification. B. Review of the EMR Specification is the responsibility of the EMR Specification Management and is outside of this SLA.
IV. **Privacy and Security**	A. A Threat Risk Assessment (TRA) and a Privacy Impact Assessment (PIA) were undertaken as requirements for HRM production implementation. B. Delta TRAs and PIAs may be undertaken when the HRM application undergoes technical design changes.

2.2 Service Requests

2.2.1 Clinician enrollment / de-enrollment to receive reports from a hospital

Service Preconditions

A. Hospital	A. The identified hospital is a registered HRM facility and the HRM interface has been successfully deployed;
B. Clinic	A. The clinic uses an EMR that conforms to OntarioMD EMR Specifications 4.1 or higher; B. The clinic's required secure folder has been established; and C. The clinic's EMR has been configured to use the HRM service.
C. Clinician	A. A CPSO or CNO number; B. The required access rights and permissions for all interrelated IT systems managed within the hospital or clinic;

2.2.1.1 Service Provisions: Enrollment Services

This service provisions the HRM service to clinicians who are:

- Enrolling for the first time for HRM service; or
- Are established HRM subscribers, and are requesting to receive reports from additional hospital(s).

A clinician who wishes to enroll emails the Enrollment Form to the eHealth Ontario Service Desk. The Enrollment Form requires the following information to enable HRM services: Clinician Name, CPSO/CNO number, the name of the hospital from which the clinician wishes to receive reports and the name of the clinician practice where the clinician will receive reports via the clinic's EMR.

Responsibilities	**Details**
A. **Clinic**	• Initiate enrollment request by calling eHealth Ontario Service Desk at phone number: 1.866.250.1554 • Confirm that the requesting clinician is an EMR user with appropriate rights and permissions.
B. **OntarioMD**	• Verify the CPSO/CNO number via the CPSO/CNO website; • OntarioMD will interface with hospitals live on HRM on behalf of the enrolling clinician and provide the necessary information for the hospital to execute their processes and procedures to attach the clinician to the hospital's required IT systems. • OntarioMD will review the HRM User Directory that the requesting clinician's CPSO or CNO number exists or does not exist within the directory. The HRM User Directory is used to identify and enable HRM to deliver a report to the clinic's secure folder. ○ If the CPSO/CNO number does not exist in the HRM User Directory, OntarioMD will: ▪ Add the requesting clinician to the HRM User Directory; ▪ Pending confirmation from the hospital that the clinician is eligible to receive reports electronically, add the hospital to the clinician's list of facilities from which they can receive reports; and • Once HRM enrollment has been completed, the eHealth Ontario Service Desk will inform the requesting clinician that the HRM service has been established. • OntarioMD will distribute a list of HRM subscribers (Physicians and nurse practitioners) to hospitals using the "New HRM Clinician Report".
C. **Hospital**	• Define internal hospital policy to determine the process for adding new HRM clinician subscribers to hospital distribution systems. • If a hospital decides not to add a particular clinician to its HRM distribution, the hospital is not obliged to inform OntarioMD; however, an alternative distribution method must be maintained for that clinician.

2.2.1.2 *Service Provisions: De-Enrollment Services*

- When a clinician becomes ineligible or chooses to stop receiving reports through HRM (e.g., no longer works at an HRM-subscribed practice), the clinician or clinic administrator phones eHealth Ontario Service Desk at phone number: 1.866.250.1554 to initiate the service request.
- As soon as OntarioMD is informed, OntarioMD is responsible for informing hospitals using the "Delete HRM Subscriber" request of this change immediately to ensure the clinician continues to receive reports through appropriate distribution method.
- The hospital must immediately act on the "Delete HRM Subscriber" request received from OntarioMD.

Responsibilities	**Details**
A. **Clinic**	• Initiate de-enrollment request immediately by calling eHealth Ontario Service Desk at phone number: 1.866.250.1554
B. **OntarioMD**	• Validate within the HRM User Directory that the requesting clinician's CPSO/CNO number exists within the directory and deactivate the user. • OntarioMD will immediately inform all hospitals live on HRM to remove the clinician from the hospital's HRM delivery system using the "Delete HRM Subscriber" request. • Once HRM de-enrollment has been completed, the OntarioMD Service Desk will inform the clinician that the request has been completed.
C. **Hospital**	• Hospital's operational resource immediately updates hospital report distribution table to ensure clinician receives reports through appropriate alternative means instead of HRM.

2.2.1.3 Service Limitations

The service level is contingent on the parties involved to fulfil their responsibilities in a timely manner and to ensure that appropriate controls are enabled.

2.2.1.4 Information requests for report types provided by a hospital

Upon request, OntarioMD will provide an outline of the various report types for a specific hospital.

2.2.1.5 HRM Service Transaction Report requests.

IT Service Transactional Reports are available in accordance with PHIPA HINP requirements:

“The provider shall to the extent reasonably practical, and in a manner that is reasonably practical, keep and make available to each applicable health information custodian, on the request of the custodian, an electronic record of,

i. all accesses to all or part of the personal health information associated with the custodian being held in equipment controlled by the provider, which record shall identify the person who accessed the information and the date and time of the access, and

ii. all transfers of all or part of the information associated with the custodian by means of equipment controlled by the provider, which record shall identify the person who transferred the information and the person or address to whom it was sent, and the date and time it was sent.”

To request a service transaction report, please contact the eHealth Ontario Service Desk.

2.3 Service Exclusions

2.3.1 Identity and access management for hospitals and clinic IT systems

OntarioMD will inform hospitals regarding HRM enrollment and de-enrollment requests. It is the responsibility of the hospitals and clinician practices to manage the requesting clinician's access to their various IT systems that support HRM services such as Hospital Information Systems and HRM Integration Engines and EMRs.

Report handling services including re-direction, re-sending/re-transmission, re-formatting, etc.
Due to the nature of the service and its content, report handling services such as re-direction, re-sending/re-transmission and re-formatting are excluded.

2.3.2 Report content augmentation, deletion or edits

Due to the nature of the service provided, HRM will not augment, delete or edit report content.
HRM Services processes the message from the hospital to meet report structure requirements as per the EMR message standard.
HRM Services will manage the HRM message header as per deployment configuration to ensure successful delivery.

2.3.3 Deletion of reports within the HRM secure folder

It is the responsibility of the EMR to delete a report after the report has been received by the clinic's EMR.

2.3.4 Data management services - responsibilities, conditions and limitations

A. OntarioMD owns the system logs and non-PHI data within these logs. OntarioMD is not responsible for, nor does it have access to PHI, unless required by an incident/change for assessment and resolution purposes.

B. HRM is not a data repository. HRM monitors and notifies the OntarioMD IT support team if reports have not been picked up within 24 hours. The OntarioMD IT support team will interface with the affected clinician practice.

C. EMR systems are required to delete all reports after successful retrieval from HRM.

D. Any reports that have been placed in a clinic practice's designated secure folder for longer than 28 days will be deleted after communications to notify the clinician practice that the reports have not been picked up. OntarioMD will contact and inform the clinic that reports are waiting to be retrieved. In the event that a report has been purged and needs to be recovered, the clinic is responsible for contacting the hospital to request that the hospital re-send the report. The clinician or delegate will contact the hospital to request that the report be re-sent.

2.3.5 Deployment services including EMR configuration and EMR related technical support.

2.4 Service Levels

2.4.1 Availability

Availability for a given period is defined as the percent of actual time during which the HRM application domain, including all components (transformation engine, user registry), was available for use or consumption, measured against the total agreed upon time the HRM application domain was to be available (the Potential Service Time) during the same period.

$$Availability = \frac{\{(Potential\ Service\ Time) - Downtime\}}{Potential\ Service\ Time}$$

The Potential Service Time is the agreed upon hours of service during the period, excluding:

- Periods of scheduled maintenance;
- Service enhancements / changes that force an outage requested and approved by the customer;
- Service disruptions due to acts of God and/or in the event of a major disaster declaration at the data centre;
- Service downtime due to eHealth Ontario infrastructure downtime;
- Service downtime due to HRM subscriber downtime at either end points: hospital report source systems or Electronic Medical Record;

Downtime shall only be calculated when it occurs within the Potential Service Time.

HRM Application Target Service Availability Level: 95%

2.4.2 Service Constraints & Limitations

HRM is a managed service and as such, certain operational constraints and limitations are imposed. The service availability overall is impacted by the managed services and integrated services' availability.
Entities Involved:

1. eHealth Ontario;
2. Hospitals;
3. Clinics;
4. EMR vendors;
5. Relevant third party vendors; and
6. OntarioMD.

Managed Service Conditions – eHealth Ontario Infrastructure

OntarioMD has an infrastructure hosting agreement with eHealth Ontario. The following is an excerpt from that agreement relevant to the HRM service.

A Service Stabilization Period [1]that will begin when the Hosting Service goes live and will continue for ninety (90) calendar days. During this period, eHealth Ontario will work with OntarioMD to ensure that the implementation is stabilized to meet service expectations and there are no residual risks impacting service delivery. The Service Stabilization Period clock will restart when the solution has any major infrastructure changes.

The Service Level Baselining Period[2] will begin at the completion of the Service Stabilization Period and will continue for one hundred and eighty (180) calendar days. During this period eHealth Ontario will track the performance against the Target Service levels and at the end of the period, document service level measures acceptable to both parties. Formal reporting of performance against these agreed upon service levels will come into effect at the completion of the Service Level Baselining Period. eHealth Ontario will use commercially available means to achieve the agreed upon service levels.
NOTE: Once approved, this SLA will be placed under Service Level Management process change control and will be subject to documentation and content management procedures.

Communications Guideline

Notification and information exchange with regard to various infrastructure maintenance and service changes is a critical requirement for service availability. The following table outlines notifications and information exchange requirements.

[1] *Service Stabilization Period is a defined period of time to commence immediately after go-live, during which service support personnel identify and address issues within the service components (infrastructure, application, etc.) such that the operation of the service may reach a stable state for ongoing operation.*

[2] *The Service Level Baselining Period is a defined period of time during which the service is monitored to determine reasonable expectations for achievement of specific service level targets. The Service Level Baselining Period must be preceded by a stabilization period to ensure that instability in the solution components do not impact the baselining exercise.*

Availability	Timeframe	Notes / Description
Production HRM system availability	Scheduled uptime – 24 hours a day, 7 days a week including statutory holidays Target: 95%	Excluding scheduled downtime
Production HRM system scheduled maintenance (Planned downtime)	Monthly: Sunday 12:00AM to 6:00AM or as agreed with involved entities. Required lead time notification: minimum 10 business days	Notification and information exchange as per the instructions in the Operations User Guide
Production HRM system unplanned downtime	Immediately (e.g., emergencies)	Notification and information exchange as per the instructions in the Operations Guide. (based on priority and urgency/impact – fast tracked changes)
Hospital HRM interrelated systems downtime/changes that result in a downtime greater than 24 hours	Required lead time: minimum 10 business days	Assurance of integrity and consistency of connection to HRM is the responsibility of the hospital. OntarioMD is available for testing on request. The lead time provided is the minimum time estimate which may be exceeded due to the magnitude and extensibility of the change. This estimate excludes the time and parties engaged to analyze, design and test the change request. All changes and/or downtime to be scheduled and impacted parties to be notified accordingly.
Clinician practice's EMR instance or EMR ASP downtime/changes	Required lead time: minimum 10 business days	Assurance of integrity and consistency of HRM EMR specifications and its interface to HRM secure message folder is the clinician practice's responsibility. OntarioMD HRM is available for testing on request. The lead time provided is the minimum time estimate which may be exceeded due to the magnitude and extensibility of the change. This estimate excludes the time and parties engaged to analyze, design and test the change request. All changes and/or any system downtime, including during clinic shut down, to be scheduled and impacted parties to be notified accordingly.

SECTION 3 IT SERVICE MANAGEMENT (ITSM) – SERVICE OPERATIONS PROCESSES

eHealth Ontario and OntarioMD follow the standard ITIL V.3 framework.

3.1 Service Request Fulfillment

eHealth Ontario is the **single point of contact** for service requests related to:

A. Clinician enrollment and de-enrollment to receive reports from a hospital;
B. Information requests regarding report types provided by a hospital; and
C. Ad-hoc transactional/audit report requests.

Support Business Hours:	24 hours a day / 7 days a week / 365 days a year
Service Phone Number:	1.866.250.1554
Service Email:	servicedesk@ehealthontario.on.ca

**Note: The primary contact method for end users to report an incident to the eHealth Ontario Service Desk is by telephone. There is currently no SLA for incidents opened at the eHealth Ontario Service Desk via email.*

3.2 Incident Management

Incident management is the process for managing the lifecycle of all Incidents. The primary objective of incident management is to return the HRM service to users as quickly as possible.

3.3.1 Terms

Incident - An unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted the service is also an Incident.

Incident Identifier – an individual or entity that identifies the incident.

Incident Record - A record containing the details of an incident. Each Incident Record documents the lifecycle of a single Incident.

3.3.2 Support Contacts

The eHealth Ontario Service Desk is the **single point of contact** with end users for incident management for the Hospital Report Manager application. The eHealth Ontario Service Desk is responsible for receiving incident calls from the incident identifier and engaging either the OntarioMD service desk or eHealth Ontario's Technical Operations Centre and Tier 2 or Tier 3 support for recording, investigation and resolution.

Support Business Hours:	24 hours a day / 7 days a week / 365 days a year
Service Phone Number:	1.866.250.1554
Service Email:	servicedesk@ehealthontario.on.ca

**Note: The primary contact method for end users to report an incident to the eHealth Ontario Service Desk is by telephone. There is currently no SLA for incidents opened at the eHealth Ontario Service Desk via email.*

3.3.3 Scenarios

3.3.3.2 Hospitals sending reports to HRM

Hospitals are significant stakeholders to identify and address situations where the flow and validity of reports to HRM are continuously or intermittently dropped or disrupted.

A. Hospitals are required to call the eHealth Ontario Service Desk with regard to any planned/unplanned interrelated system outage (HIS, Integration Engine, connectivity to HRM) that they expect to occur for an extended period of time. Incidents of this type are classified as Priority Level 1 and require escalation to the impacted parties. Hospitals are responsible for ensuring the right resources are engaged for remedial action.

B. For connectivity interruptions or planned or unplanned service degradation of sending services that:
   a. Exceed 24 hours in duration; and
   b. Have not been communicated to the eHealth Ontario Service Desk by the hospital:

   OntarioMD will communicate with the hospital and share observations and required information.

3.3.3.3 HRM system

HRM processing interruptions exceeding two (2) hours are classified as Priority Level 1 and need to be communicated by OntarioMD during regular business hours to all parties impacted.

3.3.3.4 Clinician practices receiving reports from HRM

Clinics are significant stakeholders to identify and address situations where the flow and validity of reports from HRM to the clinic's EMR are continuously or intermittently dropped or disrupted. Clinics are required to report any related impact or connectivity issues. For issues and incidents related to the data management within their respective EMRs, the clinics are to manage these issues with their support vendor.

3.3.3.5 ASP operator interfacing with HRM

An Application Service Provider (ASP) configuration is differentiated from other EMR instances as a single interface connection as it shared by clinician practices to retrieve HRM reports from their clinic's designated secure folder. The ASP operator will need to work closely with affected subscribers to resolve any outages caused by the ASP offering or its inability to retrieve reports from a designated secure EMR folder.

3.3.3.6 Roles & Responsibilities

Role	Tier	Description / Responsibilities
Incident Identifier	N / A	As the individual or entity that identifies a service interruption or reduction in service, responsible to escalate to eHealth Ontario Tier 1 for HRM related issues.
eHealth Ontario – for HRM related issues only	1	Initial triage of HRM requests/incidents/events based on information sheet; create ticket (standard requests, information requests, incidents) from information received from incident identifier. This includes: • Filling out investigation form based on defined criteria • Assessing and assigning priority (severity/impact/urgency criteria) • Resolve and close ticket (for standard and information requests) • Update ticketing system knowledge base • Update and obtain feedback from incident identifier regarding the incident (resolved, escalated, etc.) • If not a standard/information request, incident to be escalated to Tier 2 • Provide Service Desk reporting
OntarioMD – for HRM related issues only	2	Triage Tier 2 incident request, including: • Assess impact and assign/confirm priority, resolve Tier 2 requests,/incidents, close OntarioMD ticket , inform Tier 1 **OR** • Initiate OntarioMD Incident/Change Management/RFC process, as required • Implement and close ticket **OR** • Escalate to/Inform Tier 3, as applicable • Monitor resolution, close ticket, inform Tier 1 • Provide Service Desk reporting Resolution: As per the request/incident priority and complexity
3rd Party Vendor for OntarioMD – for HRM related issues only	3	Identify or receive request, Initiate triage, create ticket in system, fill out investigation form. Then, **either**: • Assess and assign priority (severity/impact criteria) • Resolve Tier 3 requests and incidents • Inform Tier 2 • Close ticket **OR** • Initiate Change/Release Management, as required • Carry out impact assessment • Inform Tier 2, obtain approval • Implement fix/work-around • Close ticket • Provide monthly reporting (Service Desk) • **SUPPORT**: Third Party – based on agreement Response: 30 minutes Resolution: 10 business days

3.3.3.7 Incident Management Priority Levels

Definitions

Priority – The relative importance of an Incident. It is based on the impact to the service and the urgency for the incident to be resolved. It is used to identify required times for actions to be taken.

Response Time – The target measure of the time taken to respond to an individual or entity regarding a query or report of an incident.

Resolution Time – The target measure of the time taken to restore services to prior levels of operation. The measurement is from the time that the incident ticket has been entered into the Incident Ticketing System.

Priority (P)	Definition	Response Time	Resolution Time	Description
P1	Critical	30 minutes	3 business days	Production system and application failure that prevents HRM from functioning and is impacting internal and external user access
P2	High	30 minutes	5 business days	Production degradation could interrupt or stop part or all the services within 24 hours and is impacting several internal or external users. This includes system degradation or malfunctions such as user password resets, user account management, etc.
P3	Medium	30 minutes	10 business days	Functionality Issues causing operational impact, but there is a work-around or a fix can wait; issues affecting a single user
P4	Low	30 minutes	15 business days	Non-essential functionality issues, enhancements, non-essential content, or non-essential issue

3.3 Problem Management

Overview

Problem management is the process for managing the lifecycle of all problems. The primary objectives of problem management are to prevent incidents from happening, and to minimize the impact of incidents that cannot be prevented.

3.4 Change Management

The primary goal of Change Management is to protect the live environment from unintended impacts as a result of changes made to the various systems, applications, and equipment operating to deliver HRM services.
All entities involved in the delivery of HRM services are required to communicate any system, report interface or related connectivity changes or planned system outages in advance in accordance with the agreed upon IT processes, as outlined in the Operations User Guide.

3.5 Business Continuity

The entities involved are required to manage their own business continuity governance, requirements, processes and recovery procedures.

3.6 Service Restoration

Service restoration processes must be coordinated between all parties impacted, including OntarioMD, to ensure the impact on load balancing and systems processing is monitored and managed. There are two scenarios.

A. Where reports received by HRM up to 28 days before the outage, OntarioMD will endeavour to restore these reports for a clinician practice EMR to retrieve; and
B. Where reports that were intended to be sent or were queued to be sent, but not delivered (remain within HIS domain) due to the system outage will be coordinated with OntarioMD given the volume of reports after restoration.

After the restoration of service, if any individual reports identified as not received by the clinic’s EMR, the clinic is responsible for contacting the hospital to re-send the required report.

OntarioMD is available to assist in monitoring and tracking service processing within the HRM system domain and can track the reports end-to-end on request.

SECTION 4 SLA MANAGEMENT ELEMENTS

4.1 Governance

OntarioMD is responsible for governing and managing this SLA.
Any changes to this agreement may require changes to associated documents or any other agreements that have been, or will be, signed with the involved parties, as well as enabling technology third party vendors.

Entity: OntarioMD

Role	SLA Management - Accountability & Responsibility
Director, Product Management	Overall executive accountability for the process and associated information and decisions related to HRM as a product and service.
Director, Physician IT Services	Executive sign off/approval of content and associated service level commitments attributed to service offerings and ITSM processes.
Service Desk	Provides HRM support, as applicable.
Applications Manager	Provides HRM application technical support.
Manager, Operations & Support	Assists with the verification of service level commitments and associated reporting of metrics and performance indicators at the technology level.
Service Management	Reviews service definitions and process implications.

4.2 SLA Lifecycle, Reviews & Change Process & Reporting

4.3.1 Reviews & Change Process

This SLA will be reviewed on a regular basis or at the request of a subscriber. If changes are required, OntarioMD will determine the disposition and determine any levels of endorsement needed to execute the amendment based on the results of the analysis, including acknowledgement by the requesting party and further review if necessary with other affected parties.