EMR Health Report Manager (HRM)

Connectivity Requirements

June 15, 2021

Document Version & Status: 2.2 – Final

Table of Contents

1. INTRODUCTION

1.1 Purpose and Scope

The purpose of this document is to outline the specifications for an Electronic Medical Record (EMR) Offering to connect to OntarioMD's Health Report Manager (HRM) to retrieve health reports. The scope of the document includes software components, connectivity protocols, message formats, content, logging and auditing.

2. CONNECTIVITY TO HRM AND OPERATIONAL REQUIREMENTS

An EMR vendors' only technical interface with OntarioMD will be with the OntarioMD sFTP server. This server will be available over the Internet during testing but over the Ontario Health Digital Services (OHDS) Managed Private Network (MPN) or Internet for production.

> The majority of EMR instances will connect over the Internet. Some EMR instances might be routed over the OHDS MPN in situations where the EMR instance is deployed in a clinic that is located within a sending facility.

2.1 EMR and Physician Registration

> The following guidance from 2011 is no longer valid.
>
> *Registration for HRM involves two steps in an operational environment:*
>
> 1. *Registration of an EMR instance with OntarioMD*
> 2. *Enrollment of Physicians with their participating Hospital*
>
> OntarioMD Practice Management Consultants are responsible for working with EMR vendors and clinicians to register them with HRM. If a clinic does not know who their Practice Management Consultant is they can send an email to report.manager@ontariomd.com

2.1.1 Registration of EMR instance with OntarioMD

An EMR instance must be registered with OntarioMD to participate. The EMR instance administrator will supply the following information to OntarioMD by completing a standard form to be provided:

- Name of EMR instance (i.e., Barrie Family Health Team)
- IP address of the Instance
- EMR location name, Street Address, city, postal
- Name 1 – lead physician/nurse Contact Name 2 – local technical support
- Number 1 – lead physician/nurse Contact Number 2 – local technical support
- Contact Email 1- lead physician/nurse
- Contact Email 2 – local technical support
- Physicians associated with using the EMR (CPSO IDs, name, clinic address, email address, phone number)
- Vendor Name (e.g., EMR Software Inc.)
- Vendor Contact Name
- Vendor Contact Email
- Vendor Support Phone Number

Upon receiving this information, OntarioMD will:

- Create the EMR instance username on the sFTP server
- Create the EMR instance folder structure for the EMR, including sub-folders for hosted EMR clients if required
- Register the EMR instance
- Associate the clinicians with the EMR instance
- Provide the EMR vendor and/or administrator with the username and required keys

2.1.2 Enrolment of Physicians with a Participating Sending Facility

⚠ The following guidance from 2011 is no longer relevant.

"Physicians who are authorized by a particular hospital to receive electronic delivery of hospital reports are to provide an enrolment form to the hospital. The enrolment form includes the following information:

- *First Name*
- *Last Name*
- *CPSO #*
- *OHIP Billing Number*
- *Office Address*
- *City*
- *Postal Code*
- *Office Number*
- *Fax Number*

Once the hospital has completed the enrolment, notification is to be sent to OntarioMD and the clinician group's EMR vendor. OntarioMD and the EMR vendor will then ensure that the clinician is set up in the HRM directory and the EMR instance."

OntarioMD Practice Management Consultants work with clinicians (e.g., physicians and nurses) to enroll them in HRM. Once complete OntarioMD notifies sending facilities about the clinician enrollment. Hospitals may take up to two weeks to process this notification.

3. EMR CONNECTIVITY REQUIREMENTS

3.1 sFTP Client Software

Once registered, an EMR instance's only technical interface with OntarioMD will be an SSH client connecting to an sFTP server.

OntarioMD will not provide nor dictate which SSH client the EMR instance uses. Regardless of the client chosen, the EMR instance is responsible for automatically polling the sFTP server for new messages and removing messages from the sFTP server once downloaded. This process should occur no more than every 30 minutes and no less often than every 24 hours.

> ⚠ Automatic polling should be designed to occur continuously every day (i.e., "24 x 7") and should not require a user to be logged into the EMR for the automatic polling to occur as this may cause significant issues.

The auto-polling function should automatically reconnect if disconnected. This will account for an OntarioMD maintenance window, sFTP server unavailability, or files not found issues.

Each EMR instance will connect to the sFTP server from a secure network with a static IP address. IP Lockout will be enabled on the sFTP server meaning only the registered EMR instance's IP address will be recognized as valid. Please see Section 4 - NETWORK CONNECTIVITY for more information.

> ⚠ EMR vendors that offer local EMRs should note that they may need to advise clients to work with their IT staff and/or internet service provider to ensure their access to the internet is configured with a single static IP address.
>
> EMR instances (e.g., a local EMR Offering at a clinic or a hosted EMR Offering) are NOT allowed to use multiple IP addresses to connect to the sFTP server.

3.2 sFTP SERVER CLIENT AUTHENTICATION

> ⚠ The following guidance from 2011 is no longer valid.
>
> *"OntarioMD Hospital Report Manager will expose an sFTP server to the Internet or the OHDS MPN as appropriate. The registered EMR vendor must authenticate against the sFTP server using the SSH protocol."*
>
> It has been replaced with the following:
> - EMR instances will primarily connect to the sFTP server over the internet using the SSH2 protocol.
> - The EMR instance will be assigned an sFTP username to connect to the HRM system on the sFTP server.
> - The sFTP username should be configurable within the EMR user interface depending on the EMR deployment type, as hosted EMR Offerings and local EMR Offerings may have different methods for identifying and associating EMR instances with clinics.
> - sFTP username should not be hardcoded in the EMR instance.

Once the secure channel is negotiated and the user is authenticated, files can be transferred through the secured SSH pipeline using sFTP.

SSH keys MUST not be hardcoded in the EMR instance. OntarioMD SSH keys can change annually, or at any time if a security issue arises or if the systems environment changes. Advance notice will be sent to related parties. Only an authorized and named EMR vendor of a hosted EMR Offering or an EMR administrative user should be able to change the new keys with minimum effort.

These keys should only be available to a single named user with a second backup named user who is responsible for keeping them in a secure place.

3.3 sFTP Server Folders, Files and Encryption / Decryption

⚠ The following guidance from 2011 is no longer valid.

"Each registered EMR will have a dedicated folder hierarchy similar to the following:

- */EMR1/Production/*
- */EMR1/Test/*

The registered EMR (EMR1 as depicted above) folder will be configured as the root folder for the authenticated EMR user. The exact name will follow a standard naming format provided by OntarioMD and will reflect the physician group name.
A hosted EMR implementation may have more sub-folders in order to match each physician group to the hosted EMR instance. Example:

- */EMR1/Production/FHT1"*

Each EMR instance will be assigned a separate sFTP folder path. EMR instances should be configured to only download files from the folder path provided by HRM and should not attempt to download files from any other folders.

Each EMR instance or implementation will have restricted access to its own folders or containers at the HRM servers.

The authenticated EMR user will be granted Read, List, Delete, and Rename rights to the files in their folders.

⚠ For clarity, it is expected that EMR Offerings are designed to perform these actions automatically without requiring the EMR user to perform the file deletion or renaming.

All files waiting for the EMR to download will be encrypted. OntarioMD will provide the necessary EMR instance decryption key (128-bit AES). **No encryption/decryption keys should be hardcoded in the application**. These keys should be available to a single named user with a backup user who is responsible for keeping them in a secure place.

⚠ The following guidance from 2011 is no longer valid.

"All files awaiting EMR downloading will take the following format: <ProcessedDate>_<sendingFacility>_<reportType>_<reportNumber>_<messageDate>_<cpsoID>.xml
Example: 20090904234559123_ ABC _DI_1234567_200909041234_4321.xml"

The EMR Offering **should not validate** the file name of the XML report or on any component of the file name. The naming convention of the file name and extension may change at any time. OntarioMD is under no obligation to notify EMR vendors of such changes.

These XML files will conform to the most current EMR HRM XML schema specifications.

⚠ It is recommended that EMR instances validate the downloaded HRM XML files against the HRM XML schema.

sFTP Folders will be monitored by OntarioMD. To support a consistent approach to the sFTP folder management and audit logging, we recommend the following process be followed as part of the EMR's message retrieval process.

- The auto-polling process to be set at no less than 30-minute intervals
- An EMR also requires a manual polling and retrieval function for administrator support
- It is recommended that files to be retrieved in the sFTP folder be renamed by the EMR vendor with an appropriate file name extension to mark the files that will be retrieved
- The EMR system will retrieve only renamed files
- The EMR system ensures the files have been successfully retrieved
- The EMR system can then delete the renamed files

⚠ The EMR system MUST delete the HRM XML file from the sFTP server after it has been downloaded to the EMR system.

⚠ The following information from 2011 is for awareness only:

The sFTP audit log will log the following events: by user, system, time, date,

- Polling and access to the folder
- File save to the folder
- File rename
- File retrieve
- File delete
- Log off sFTP server

The sFTP server will send an alert to OntarioMD and the clinic's technical support contacts if a file remains on the server for more than 24 hours.

Any file that remains on the server for more than 28 days may be deleted by OntarioMD to ensure privacy and security requirements are met.

⚠

- EMR vendors need to decide what to do if an EMR Offering downloads an HRM file that fails to be decrypted or validated against the HRM XML schema. There have been issues in the past where EMR Offerings were designed to leave rejected HRM files on the sFTP server – with their original file name or with an updated file name - which resulted in the file being continuously polled and rejected by the EMR Offering.
- It is recommended that EMR Offerings store the HRM files that failed to be decrypted or validated against the HRM XML schema and allow the EMR administrator access to those files to assist with troubleshooting.
- It is recommended that EMR users be alerted to validation errors with clear and easy-to-understand messages that allow them to decide as to whether or not to save the invalid HRM file to the physician inbox and/or patient chart. Example types of errors may include:
    - sFTP server unavailable or unreachable
    - polling mechanism failure
    - sFTP account locked out or connection denied
    - unable to decrypt the XML file
    - XML file validation error
    - EMR specific processing errors on valid XML files

4. NETWORK CONNECTIVITY

Each registered EMR will have network access to OHDS's Ontario Managed Private Network (MPN) or Internet connectivity to reach OntarioMD HRM servers.

> ⚠ The majority of EMR instances will connect over the Internet. Some EMR instances might be routed over the OHDS MPN in situations where the EMR instance is deployed in a clinic that is located within a sending facility.

If using an existing OHDS circuit, bandwidth may vary. For new EMR connectivity, a minimum of five Mbps download speed is required.

> ⚠ The following guidance from 2011 has been revised.
>
> *"Network connectivity is to be protected by firewall security that supports Universal Threat Management (UTM) and Deep Packet Inspection (DPI)."*
>
> Network connectivity is to be protected by firewall security that supports Universal Threat Management (UTM). The firewall does not need to have Deep Packet Inspection (DPI) because the connection is encrypted.

A firewall with UTM is recommended for existing local EMR implementations, but mandatory for hosted EMR and new local EMR implementations. Firewalls must be monitored and updated on a regular basis.

The machine accessing HRM servers over SSH must be physically secure and accessed only by a limited number of authorized users. This machine is expected to have a business-class OS and be protected with an appropriate firewall, anti-malware software and be updated on a regular basis.

Vendors of hosted EMRs must provide more details in advance about their EMR connectivity when they support multiple instances from a single IP address.

> ⚠ The following guidance from the 2011 publication is no longer valid.
>
> *"If an ASP (also known as Hosted) EMR vendor setup shares the same sFTP folder for several physician groups, then this ASP vendor will need to present a signed agreement with each of these groups covering the required privacy and security measures related to data sharing."*
>
> Folders will never be shared; they will always be uniquely named per the clinic.

Each hosted EMR vendor will be assigned a different decryption key.

Changes to EMR network connectivity may require up to 10 business days to process. Therefore, sufficient notice is required.

5. LOGGING AND AUDITING

OntarioMD is responsible for the logging and auditing of all messages from the sending facility to the EMR. EMR vendors are required to log enough information to assist OntarioMD if and when requested.

> ⚠ The following text was included in the 2011 publication. The Personal Health Information Protection Act (PHIPA) has undergone changes since this text was provided. EMR vendors must ensure their EMR Offerings remain compliant with PHIPA.
>
> *"EMR instances must understand and comply with the Personal Health Information Protection Act (2004) (PHIPA) of Ontario. A subset of these requirements states that*:
>
> *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. This could be a request to assist with the tracking of a reported missing message, improperly routed message, etc.*
>
> *The full Act can be accessed at:*
> *http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_040329_e.htm."*

At a minimum, all IDs received by the EMR instance (i.e., Message IDs, Sending Facility IDs and CPSO IDs) are critical to this requirement, as well as dates and times when messages were handled by the EMR instance.

The sFTP server performs logging and auditing support including, but not limited to:

- Successful and failed login attempts
- Files uploaded, downloaded, and renamed
- Other administrative functions

6. ADDITIONAL CONSIDERATIONS

⚠ **Additional Considerations**

1. HRM XML files are encoded in UTF-8. EMR vendors should anticipate that HRM reports might contain any character encoded in UTF-8.
2. The EMR Offering should be designed to consider variations in the number and size of XML files available to a clinic. For example, a large clinic may have 500+ files waiting in the sFTP folder at any given time, and the files may typically range in size from 2 KB to 12 MB. EMR vendors should consider these variations when designing the logic for downloading, decrypting, validating and performing other file processing activities.
3. Some text-based reports might contain extremely long lines of text that are difficult to display in a user-friendly manner in the EMR Offering. It is recommended to ensure the EMR Offering wraps report text in a manner that does not obscure or omit any content and is logically laid out. Forcing the EMR user to horizontally scroll long lines of text is considered a bad practice.