OntarioMD

Electronic Medical Records

SPECIFICATION

Hospital Report Manager

EMR Connectivity Requirements

FINAL

Date: January 31, 2011

Version: 2.0

Contents

INTRODUCTION **3**

PURPOSE AND SCOPE 3

REFERENCES 3

CONNECTIVITY TO HRM AND OPERATIONAL REQUIREMENTS **4**

EMR AND PHYSICIAN REGISTRATION 4

1. REGISTRATION OF EMR INSTANCE WITH ONTARIOMD 4

2. ENROLMENT OF PHYSICIANS WITH A PARTICIPATING HOSPITAL 5

EMR CONNECTIVITY REQUIREMENTS **6**

sFTP CLIENT SOFTWARE 6

sFTP SERVER CLIENT AUTHENTICATION 6

sFTP SERVER FOLDERS, FILES AND ENCRYPTION / DECRYPTION 6

NETWORK CONNECTIVITY 8

LOGGING AND AUDITING 8

INTRODUCTION

PURPOSE AND SCOPE

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

REFERENCES

Please refer to OntarioMD's EMR Specifications v4.0 FINAL, released January 17, 2011 and the related documents as listed on OntarioMD's web site.

You can obtain these documents by visiting www.ontariomd.ca then click on VCN and EMR Certification and then Vendor Information .

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 eHealth Managed Private Network (MPN) or Internet for production.

EMR AND PHYSICIAN REGISTRATION

Registration for the Hospital Report Manager involves two steps in an operational environment:

1. Registration of an EMR instance with OntarioMD
2. Enrollment of Physicians with their participating Hospital

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 FHT)
- IP address of the Instance
- EMR location name, Street Address, city, postal
- Contact Name 1 – lead physician
  Contact Name 2 – local technical support
- Contact Number 1 – lead physician
  Contact Number 2 – local technical support
- EMR Contact Email 1- lead physician
- EMR contact Email 2 – local technical support
- Physicians associated with using the EMR (CPSO IDs, name, clinic address, email address, phone number)
- Vendor Name (i.e. Clinicare, Practice Solutions, HealthScreen, etc…)
- Vendor Contact Name
- Vendor Contact Email
- Vendor Support Phone Number

Upon receiving this information, OntarioMD will:

- Create the EMR Instance user name on the sFTP server
- Create the EMR Instance folder structure for the EMR (including sub-folders for ASP clients, if required)
- Register the EMR Instance with the myDDS database server
- Associate the physicians with the EMR Instance
- Provide the EMR Instance vendor and/or administrator with the user name and required keys

2. ENROLMENT OF PHYSICIANS WITH A PARTICIPATING HOSPITAL

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 physician group's EMR vendor. OntarioMD and the EMR vendor will then ensure that the physician is setup in the Hospital Report Manager directory and the EMR instance.

EMR CONNECTIVITY REQUIREMENTS

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 chooses to use. 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.

The auto-polling function should automatically re-connect 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 fixed 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 the *Network Connectivity Section* within this document.

sFTP SERVER CLIENT AUTHENTICATION

OntarioMD Hospital Report Manager will expose an sFTP Server to the Internet or the eHealth MPN as appropriate. The registered EMR vendor must authenticate against the sFTP server using the SSH protocol. The server used will be the WS_FTP server with a DSA host key with SSH from IPSWITCH (http://www.ipswitchft.com/products/ws_ftp_server/) or a similar product.

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

No SSH keys are to be hardcoded in the application. OMD keys will be changing annually, or at anytime if a security issue arises or if the systems environment changes. An advance notice will be sent to related parties. Only an authorized and named EMR ASP vendor or 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.

sFTP SERVER FOLDERS, FILES AND ENCRYPTION / DECRYPTION

- 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.

- An EMR ASP implementation may have more sub-folders in order to match each physician group to the hosted EMR instance. e.g.
    - /EMR1/Production/FHT1
- 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.
- All files awaiting EMR downloading 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.
- 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
- These xml files will conform to the most current OntarioMD EMR specifications. Please refer to the specifications located on the OntarioMD website as listed under the References section at the beginning of this document.
- sFTP Folders will be monitored by OntarioMD. In order 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 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 Folder
- The sFTP server will sent an alert to OntarioMD if a file remains on the server for more than 24 hours.

- Any file that remains on the server for more than 30 days will be deleted by OntarioMD to ensure privacy and security requirements are met.

NETWORK CONNECTIVITY

- Each registered EMR will have network access to eHealth's Ontario Managed Private Network (MPN) or Internet connectivity to reach OntarioMD HRM servers. If using an existing eHealth circuit bandwidth may vary. For new EMR connectivity a minimum of 5 Mbps download speed is required.

- Network connectivity is to be protected by firewall security that supports Universal Threat Management (UTM) and Deep Packet Inspection (DPI). This is recommended for existing local EMR implementations, but mandatory for ASP and new 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 appropriate firewall, anti-malware software and be updated on a regular basis.

- An ASP Vendor must provide more details in advance about their EMR connectivity when they support multiple instances from a single IP address. If an ASP 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.

- Each ASP EMR vendor will be assigned a different decryption key.

- Changes to EMR network connectivity may require up to 4 weeks to process. Therefore, sufficient notice is required.

LOGGING AND AUDITING

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

EMR Instances must understand and be in compliance with the Personal Heath Information Protection Act (2004) 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, Hospital 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