

EMR Data Migration

Business View

January 25, 2021

Document Version and Status: 1.1 - Final



Table of Contents

1. INTRODUCTION	3
2. EMR DATA MIGRATION BUSINESS DRIVERS	3
3. EMR DATA CATEGORIES	3
4. EMR DATA MIGRATION SPECIFICATION SCOPE	4
5. STAKEHOLDERS	5
6. EMR DATA MIGRATION USE CASE	7
7. PRIVACY AND SECURITY	9
8. AUDIT LOG	9
9. MIGRATING PATIENT RECORDS WITH ENTRIES FROM MULTIPLE PHYSICIANS.....	9
10. LARGE FILE SIZE.....	11
11. ADDITIONAL CONSIDERATIONS AND RESOURCES	11

1. INTRODUCTION

The purpose of this document is to provide readers with a general understanding of the business of migrating data from one electronic medical record (EMR) to another when changing EMR Offerings. This document describes the business objectives for EMR data migration, defines key concepts, roles and responsibilities of the stakeholders involved in EMR data migration, and guides physicians and EMR vendors when considering the migration of their EMR data.

2. EMR DATA MIGRATION BUSINESS DRIVERS

The requirement for EMR data migration originated from physicians using EMRs in their medical practice who wanted to ease their transition to a new certified EMR. Examples of business drivers for moving to a different EMR include:

- The EMR Offering is no longer appropriate for the practice’s needs
- The EMR vendor is exiting the market or merging with another EMR vendor
- A physician leaves a practice that uses an EMR and joins a practice that uses a different EMR
- The EMR vendor no longer maintains certification for the EMR Offering

3. EMR DATA CATEGORIES

EMR data is a term used to broadly describe all the data stored in an EMR. This includes data stored in databases as well as reports, images and documents that may be stored as files. Table 1 provides example categories of EMR data that EMR vendors and physicians should consider when establishing migration plans.

It is important to note that the EMR Data Migration Specification does not describe how to export and import all EMR data. The EMR Data Migration - Implementation Guide specifies some of the necessary and sufficient patient information that can be exported from one EMR Offering and imported into another to ensure some degree of continuity of patient of care. It does not cover every data category listed below.

PATIENT DATA CATEGORIES	PRACTICE MANAGEMENT CATEGORIES
Patient Demographics Family History Past Health Problem List Risk Factors Allergies & Adverse Reactions Medications Immunizations Laboratory Results (Patient) Appointments Physicians' My Clinical Notes Reports Received Care Elements Alerts and Special Needs Consults & Investigations Referrals Care Plans Activity Indexes Pain Scores Diagnostic Measurements Data in Forms & Reports Patient Letters (e.g. to employers, camps, etc.) Consent	Address Book Billing Scheduling Favourites Forms & Reports Templates Letters Templates Alerts & Notifications Audit/System Log Emails (from EMR email/messaging system) Tasks Saved Searches Boilerplate Text
SYSTEM DATA CATEGORIES	
Code Tables/Look-up Tables Interfaces User Roles and Permissions Security	

Table 1 – Example EMR Data Categories

4. EMR DATA MIGRATION SPECIFICATION SCOPE

Specifying the data structure and format for every possible category of EMR data is outside of the scope of the EMR Data Migration Specification. It should be noted that the 'exporting EMR vendor' is expected to export additional data not specified by the EMR Data Migration – Implementation Guide or provide the importing EMR vendor with a copy of all EMR data (e.g. one approach could be to provide a copy of the EMR database) to facilitate the importing of the remaining data physicians require as part of the migration.

5. STAKEHOLDERS

The following stakeholders may be involved in an EMR data migration:

NAME	DESCRIPTION	ROLES AND RESPONSIBILITY
Physician	A person qualified to practice medicine who is considered the Health Information Custodian (HIC) of the personal health information (PHI) that will be migrated as part of the EMR data migration.	<ul style="list-style-type: none"> Under the <i>Personal Health Information Protection Act</i> (PHIPA) and in the context of an EMR data migration, physicians are considered HICs and are responsible for the proper and secure retention, handling, transfer and disposal of PHI. This means physicians involved in the EMR data migration are ultimately responsible for coordinating EMR data migration activities and ensuring other stakeholders understand their roles and act accordingly to help the physicians meet their responsibilities. This includes ensuring agreements are in place with all parties involved in the EMR data migration. Ensure patient data to be migrated is current and data quality errors have been corrected prior to export. <p>Ensure imported data is complete and error free.</p>
EMR User	Any person who interacts with stakeholders of the EMR data migration, and/or interacts with the exporting or importing EMR Offering (e.g., physician's practice administrative staff, clinic manager, etc.).	Support physicians to conduct various activities in order to fulfil physicians' roles and responsibilities. This could include coordinating stakeholders involved in the EMR data migration, assisting in various EMR data migration activities, etc.
Exporting EMR Vendor	The organization that owns the EMR Offering from which the physician(s) needs to export data.	<ul style="list-style-type: none"> Exports data that conforms to the EMR Data Migration – Implementation Guide and ensures the XML files validate against the EMR Data Migration – XML Schemas prior to transferring the files to the importing EMR vendor. Exports additional data not specified by the EMR Data Migration – Implementation Guide or provides the importing EMR vendor with a copy of all EMR data (e.g., one approach could be to provide a copy of the EMR database). Answers questions about the exported data in a timely manner to support the physician and

NAME	DESCRIPTION	ROLES AND RESPONSIBILITY
		<p>the importing EMR vendor to complete the EMR data migration.</p> <ul style="list-style-type: none"> • Secures the exported data at rest and in transit until such time as the importing EMR vendor has taken receipt of the data. <p>Upon request from the physicians, provides in writing, a statement that any PHI remaining with the exporting EMR vendor has been securely deleted.</p>
Importing EMR Vendor	The organization that owns the EMR Offering into which the physician(s) needs to import data.	<ul style="list-style-type: none"> • Once received from the exporting EMR vendor, secures the imported data at rest. • Imports data that conforms to the EMR Data Migration – Implementation Guide. • Imports additional data not specified by the EMR Data Migration – Implementation Guide such as importing data from a copy of the source EMR database.
IT Service Provider	A third-party organization that physicians, importing EMR vendors or exporting EMR vendors contract with to act on their behalf during the EMR data migration.	Fulfils contractual obligations related to the roles and responsibilities of the stakeholder it represents.
OntarioMD	OntarioMD collaborates with EMR vendors to implement connectivity to certified EMRs that enhance their value.	<ul style="list-style-type: none"> • Provides a single point of contact for physicians and certified EMR vendors involved in an EMR data migration. Responds to questions related to stakeholders’ roles and responsibilities and interpretation of the EMR Data Migration Specification. <p>Maintains the EMR Data Migration Specification, including management of issues and change requests.</p>

Table 2 – Stakeholders

6. EMR DATA MIGRATION USE CASE

EMR data migration has two basic use cases:

1. Data export – Describes the participants and systems involved in exporting data from an EMR Offering into one or more files.
2. Data import – Describes the participants and systems involved in importing data from one or more files into an EMR Offering.

Figure 1 - EMR Data Migration Use Case illustrates:

- How the exporting EMR vendor interacts with the EMR Offering to generate the XML files and associated documents, reports, images, etc.
- How the importing EMR vendor interacts with the EMR Offering to import the XML files and associated documents, reports, images, etc.

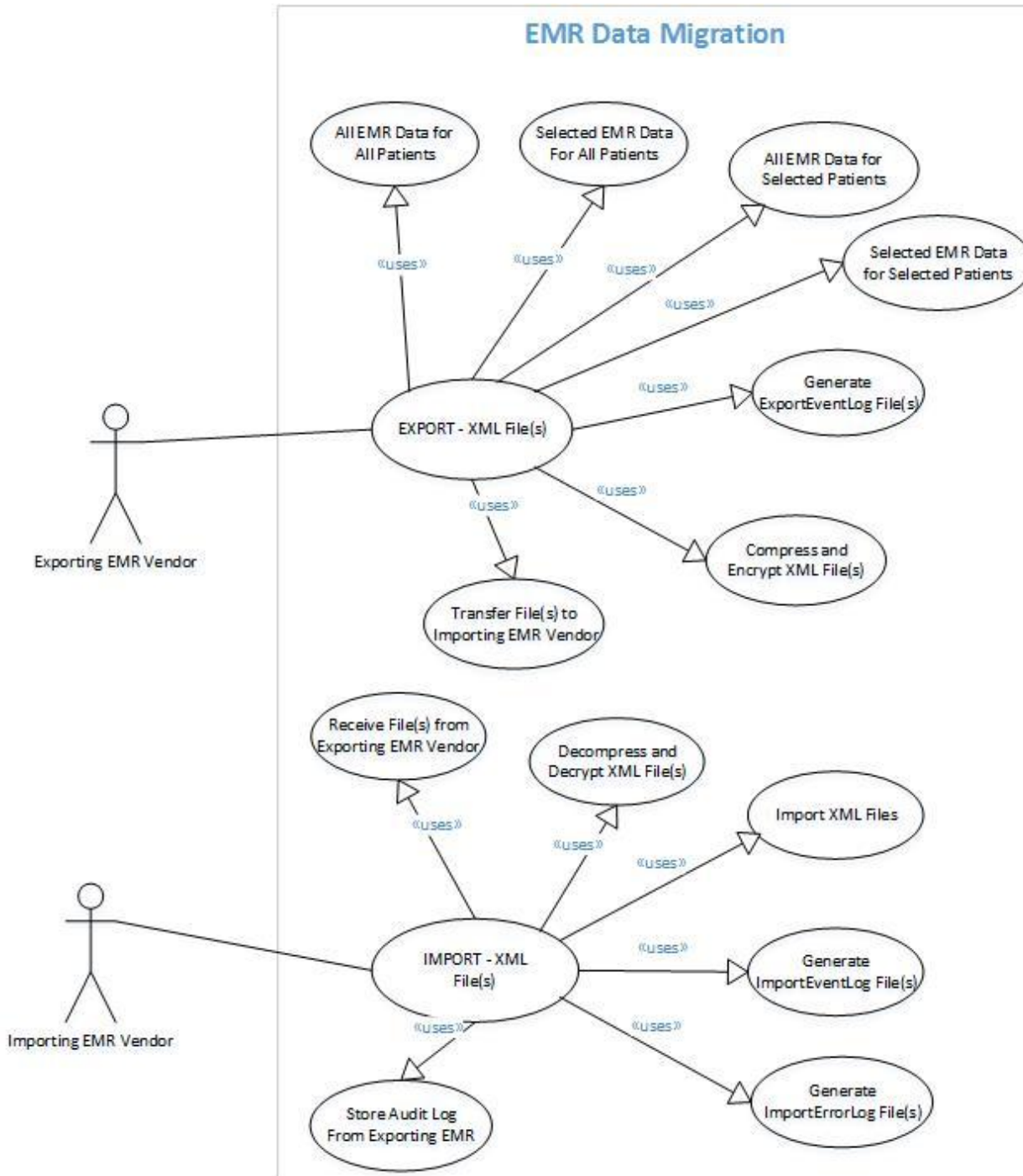


Figure 1 - EMR Data Migration Use Case

7. PRIVACY AND SECURITY

Stakeholders involved in EMR data migrations must understand their accountability for protecting the privacy and security of Personal Information and Personal Health Information as required by various laws, regulations and applicable policies and/or professional requirements. For example, under PHIPA, physicians are considered Health Information Custodians. Section 12 of PHIPA states that “A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.”¹ Section 13 of PHIPA further states that “A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner.”.

8. AUDIT LOG

The College of Physicians and Surgeons of Ontario (CPSO) Policy on Medical Records states “Where there will be more than one health professional making entries in a record, each professional’s entry must be identifiable, which may, in an EMR, be accomplished through an audit trail. Where a Physician has limited control over the content of a shared record, he or she is only accountable for his or her own entries into the record. The Physician must ensure the accuracy of the entries made into the medical record on his or her behalf by a trainee or the recipient of delegation. This may be indicated by cosigning the entry.” And “For electronic systems, there must be a functioning audit trail or record of who has accessed an EMR and what additions or edits they have made to the record over time.”²

The audit log needs to be included in the EMR migration. Physicians and vendors should discuss what type of information the audit log will contain, such as:

- Does the audit log capture information about edits (e.g., additions, changes, deletions) to a patient record, who made the edits, and when they were made? If so, does it
 - Capture the information about the record as a whole, or does it capture it for individual entries?
 - How are the people who made the edits identified in the log?
- Does the audit log include information about who viewed a patient record? If so, the same questions as above also apply.

9. MIGRATING PATIENT RECORDS WITH ENTRIES FROM MULTIPLE PHYSICIANS

Special care must be taken by physicians and EMR vendors when exporting patient data with entries made by multiple physicians because it can be tricky to determine who is the Health Information Custodian. Physicians who are a part of a practice should consult the CPSO policy, PHIPA, as well as data sharing agreements and other policies that may exist with other members of the practice in order to understand their rights and obligations for copying versus moving patient data. Physicians should consider the following scenarios and questions:

¹ Personal Health Information Protection Act, 2004, c. 3, Sched. A, s. 12 (1).

² Personal Health Information Protection Act, 2004, c. 3, Sched. A, s. 13 (1).

The physician considered to be most responsible for a patient leaves a practice, and the patient is moving with the physician to the new practice.

- Patient record only has entries from the physician considered to be most responsible.
 - An entire copy of the patient record needs to be migrated. Does a copy of the patient record need to be left with the practice and if so, should it be read only or editable? Should the migrated data be deleted (logically or physically) from the source EMR?
- Patient record has entries from one or more physicians who are not considered to be most responsible.
 - An entire copy of the patient record needs to be migrated. This includes entries made by other physicians. Does a copy of the patient record need to be left with the practice, or just the entries made by other physicians? Should the entire record or the entries that remain be read only or editable? Should any of the patient's data be deleted (logically or physically³) from the source EMR?

The physician considered to be most responsible for a patient leaves a practice, and the patient is not moving with the physician to the new practice. Since the patient is not moving to the new practice, their records should stay with the current practice and a new physician should be identified as being most responsible.

- Patient record only has entries from the physician leaving the practice that formerly had primary responsibility.
 - The physician leaving the practice should consider if a copy of the entire patient record needs to be migrated into their new EMR, or would paper copies suffice to meet CPSO policies. If a copy of the entire patient record is transferred, should it be read only or editable?
- Patient record has entries from one or more physicians who are not considered to be most responsible.
 - The physician leaving the practice should consider if a copy of the entire patient record or just the entries the physician was responsible for needs to be migrated into their new EMR. Would paper copies of the entire record or paper copies of just the entries the physician was responsible for suffice to meet CPSO policies? Should the entire record or the entries that were copied be read only or editable?

The physician who is not considered most responsible for a patient leaves a practice, but had made entries in patient records that belong to other physicians.

- Should the physician leaving the practice migrate complete patient records in which they made entries? Should they migrate only the entries they made? Should the entire patient record or the entries that were copied be read only or editable? Since the physician does not have primary responsibility for the patient, would print-outs suffice to meet CPSO policies?

Another scenario physicians need to consider during a migration is if any of the patient records contained in the EMR were in the custody of a retired physician or physician who never legally transferred custody of patient records. These situations can be challenging because of the inability to contact the physician who was

³ Logically deleted is a term used in IT to describe a situation where data is effectively deleted so that most users cannot access it, but if there was ever a need to retrieve the data (e.g., for an audit) an administrator could retrieve it. Physically deleted means the data is removed from all storage media and cannot be retrieved by anyone.

the Health Information Custodian of the records. Physicians who find themselves in these situations should review CPSO policy and contact the CPSO for guidance.

10. LARGE FILE SIZE

The file size of electronic patient records can become very large over time and impact the ability to store, encrypt/decrypt and transfer over a network. It is not uncommon for some patient records containing scanned reports and images to have file sizes measured in terabytes (TB). Some of the issues that may be encountered from large file sizes include:

- 1) Storage - Operating systems and hard drive formats place limits on the size of individual files, which can impact the ability to create the files or the ability to perform basic operations such as moving, copying or deleting the files.
- 2) Applications - Many applications, including those used to encrypt or decrypt files, might not be able to open large files or may experience performance degradation. This can impact the broader system performance depending on the application design and its relationship with the processors and memory of the system on which the application is installed.
- 3) Network transfer - Networks and their various protocols can have limitations on the upload and download speeds that can impact the performance of the data transfer. For example, a 2 TB file would take approximately five hours to transfer on a Gigabit Ethernet (1,000 Mbps Gig E) or approximately two days over a 100 Mbps Fast Ethernet connection. When multiplied by the number of files that need to be transferred, the length of time to transfer files can be measured in days or weeks, which can introduce some security risks associated with having an open connection for that long as well as performance risks if connections are interrupted.

The specific approaches for resolving the issues described above will need to be agreed to by the physician(s), exporting EMR vendor and importing EMR vendor.

11. ADDITIONAL CONSIDERATIONS AND RESOURCES

Many activities are required to ensure EMR data migrations are executed according to plan. For example, physicians need to:

- Determine what data needs to be migrated
- Decide if they need to clean up the data prior to migration
- Review EMR vendor agreements to understand costs and responsibilities for specific services
- Check data sharing agreements with others in the practice

OntarioMD provides the following documents to assist stakeholders to plan their EMR data migration appropriately:

- EMR and Data Migration Guide – a comprehensive guide for physicians to support the migration from one EMR Offering to another.
- EMR Data Migration Project Plan – a project plan template to support stakeholders to plan effectively for EMR data migrations.

Both documents are available from OntarioMD's Guidelines, Policies and Procedures web page at:

<https://www.ontariomd.ca/resource-library/policies-and-procedures>

Physicians requiring assistance with understanding their obligations under PHIPA, CPSO policy, and other legislative or regulatory requirements can contact the Ontario Medical Association Practice Management and Advisory Services, which provides a broad range of resources, services and training programs that help physicians establish and maintain successful medical practices. For more information, please visit <https://www.oma.org/sections/managing-your-practice/running-your-practice/> or contact: practicemanagement@oma.org