

EMR Privacy and Security

Requirements

September 30, 2021

Document Version & Status: 1.0 – Final



Table of Contents

1. INTRODUCTION	3
1.1 OVERVIEW	3
1.2 VERSION HISTORY	3
1.3 SCOPE	3
1.4 ASSUMPTIONS	3
1.5 RELATED DOCUMENTS, REFERENCES AND SOURCES	4
2. EMR REQUIREMENTS	5
2.1 EMR BASELINE	6
2.1.1 <i>System Access Management</i>	6
2.1.2 <i>Auditing and Logging</i>	9
2.1.3 <i>Privacy Requirements</i>	12
2.1.4 <i>Security Requirements</i>	12
2.2 EMR HOSTING	13
2.2.1 <i>Threat Risk Management</i>	13

1. INTRODUCTION

1.1 Overview

This document defines EMR requirements and provides guidance on privacy and security requirements in an Local EMR Offering and in a Hosted EMR Offering. The intended audience of this document includes business and technical implementers interested in functionality within an EMR Offering to access Provincial EHR products and services. Requirements are separated into two main sections as follows.

- **EMR Baseline** – Applicable to EMR functionality for both Local and Hosted EMR Offerings
- **EMR Hosting** – Applicable to Hosted EMR Offerings only (and not to Local EMRs)

1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2020-09-10	<ul style="list-style-type: none"> a) Initial release i) Moved requirements originally from Primary Care Baseline Specification: <ul style="list-style-type: none"> 1. PS01.XX from emr14.XX 2. PS02.XX from emr16.XX 3. PS03.XX from emr20.XX 4. PS04.XX from emr21.XX ii) Moved requirements originally from EMR Hosting Specification <ul style="list-style-type: none"> 1. PS05.XX from HST08.XX

1.3 Scope

- The requirements in this document apply to both Hosted and Local EMR Offerings. Some requirements only apply to Hosted EMR Offerings and not to Local EMR Offerings, found in the EMR Hosting section. All other sections apply to both Local and Hosted EMR Offerings.
- The requirements in this document generally apply in any health care domain.

1.4 Assumptions

- Readers have a general understanding of EMRs.
- Readers have a general understanding of privacy and security regulations within their respective business domain.

1.5 Related Documents, References and Sources

NAME	VERSION	DATE
CPSO Policies - Medical Records (College of Physicians and Surgeons of Ontario, 2020) https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Medical-Records-Management	N/A	2020-03

2. EMR REQUIREMENTS

This section consists of the EMR functional requirements pertaining to the EMR Privacy and Security Specification.

Support:

M = Mandatory. EMR offerings certified for this specification **MUST** support this requirement.

O = Optional. EMR vendors **MAY** choose to support this requirement in their certified EMR Offering.

Status:

N = New requirement for this EMR Specification version.

P = Previous requirement.

U = Updated requirement from the previous EMR Specification version.

R = Retired requirement from the previous EMR Specification version.

OMD #:

A unique identifier that identifies each requirement within OntarioMD’s EMR Requirements Repository.

CONFORMANCE LANGUAGE

The following definitions of the conformance verbs are used in this document:

- **SHALL/MUST** – Required/Mandatory
- **SHOULD** – Best Practice/Recommendation
- **MAY** – Acceptable/Permitted

The tables that follow contain column headings named: 1) “Requirement,” which generally contains a high-level requirement statement; and 2) “Guidelines,” which contains additional instructions or detail about the high-level requirement. The text in both columns is considered requirement statements.

2.1 EMR Baseline

The following requirements in this section apply to both Hosted and Local EMR Offering models.

2.1.1 System Access Management

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.01	<p>The EMR user MUST enter a password in order to access EMR Offering functions.</p> <p>The EMR Offering MUST store passwords in an encrypted format.</p>	Encryption applies to passwords managed by EMR Offering. Passwords stored and managed by the operating system are already considered encrypted and secure.	M	P
PS01.02	<p>EMR Offering MUST support passwords that include:</p> <ul style="list-style-type: none"> • Mixed case passwords • Passwords of a minimum of 8 characters • Alphanumeric characters • Special characters 		M	P
PS01.03	<p>The EMR Offering MUST have password management capabilities that can be deployed based on the EMR user discretion</p>	<p>Password management capabilities include:</p> <ol style="list-style-type: none"> a) The ability to set parameters for the number of failed login attempts within a certain period b) The ability to set time parameters for password expiry <p>This applies to all passwords used by the EMR Offering, including the operating system and all applications.</p>	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.04	The EMR Offering MUST be able to share patient data among physicians who access the same database	MUST maintain proper physician identification. Patient data MUST only be shared if permitted by practice rules.	M	P
PS01.05	Provides the capability to create roles	Need to be able to create new roles, with customized permissions. If the EMR Offering provides only pre-defined roles, this requirement is not met. Changes applied to a role mean that this change is applied to all members of that role. Multiple roles can be assigned to the EMR user.	M	P
PS01.06	There are access controls to functions based on roles	Members of a role have access/restrictions to certain screens and capabilities in the EMR Offering based on the functions assigned to that particular role. For example, the EMR Offering should ensure the merge function can be assigned to a specific user, EMR user role, or group.	M	P
PS01.07	There are access controls to data based on roles	Members of a role cannot access certain data, even though that role can access a function that uses the data. It gives control over what the role can access at the physical or logical record level.	M	P
PS01.08	There are access controls to functions based on the EMR user	An EMR user cannot use certain screens or capabilities of the EMR Offering.	M	P
PS01.09	There are access controls to data based on the EMR user	An EMR user cannot access certain data, even though that EMR user can access a function that uses the data. It gives control over what the EMR user can access at the physical or logical record level.	M	P
PS01.10	Provides different views to data for roles	Screen layout, organization, or contents can be customized for different roles.	O	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.11	Clerical staff who do not have permission to view patient medical data can enter notes into the EMR Offering	Notes entered against practice management data (e.g., patient demographics, appointments) would not meet the requirement.	M	P
PS01.12	EMR Offering MUST ensure the encryption of: <ul style="list-style-type: none"> • Passwords transmitted over a WAN. • Data that is transported across private or public networks. • Data stored offline (backups, archives, etc.) 		M	P
PS01.13	Provides the ability for multiple EMR users to access the EMR Offering concurrently	Single EMR user access to EMR Offerings is not accepted.	M	P
PS01.14	Provides the ability for concurrent EMR users to simultaneously view the same record	Refers to practice management information, as well as clinical information.	M	P
PS01.15	Provides protection to maintain the integrity of clinical data during concurrent access	To prevent EMR users from simultaneously attempting to update a record with resultant loss of data.	M	P
PS01.16	Provides a way to quickly “lock” an EMR user workstation if left unattended	The following rules MUST apply: <ol style="list-style-type: none"> a) The EMR user MUST be required to enter a valid password in order to unlock the workstation b) MUST preserve context when unlocked c) MUST be quick; a screen saver after 30 minutes is not acceptable d) EMR data MUST not be accessible 	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Acceptable solutions are: a) EMR user-initiated lock (e.g., hotkey); and b) Screen lock with a timeout period		
PS01.17	Ensures security when one EMR user is logged on at multiple workstations	MUST be able to log on to the EMR Offering through a second workstation with the same EMR user credentials without logging out of the first workstation.	M	P
PS01.18	Ensures security when several EMR users use the same workstation in quick succession to access: a) A single patient record or b) Multiple patient records	MUST be able to log on to the EMR Offering with a second set of EMR user credentials without logging out the first EMR user. The second EMR user cannot see the first EMR user's data and vice versa. If an EMR Offering uses operating system features (e.g., user profile switching) to meet this requirement, then a version of the OS that provides this feature MUST be included as part of the EMR.	M	P
PS01.19	Supports Remote Access through internet connections using Virtual Private Network (VPN)	MUST be able to use all EMR functions when connected remotely. A VPN MUST be supported to offer remote connections (e.g., access from home).	M	P

2.1.2 Auditing and Logging

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS02.01	There will be a complete audit trail of medical records in accordance with the CPSO requirements. Each patient record in the EMR Offering MUST have a distinct audit trail.	All activity (i.e., data viewed, updated, deleted) against medical records maintained by the EMR MUST be captured in the audit trail. The audit trail MUST capture: a) The date and time of the activity b) The EMR user who accessed the data c) Any changes in the recorded information	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		<p>d) Preserves the original content of the recorded information when changed or updated</p> <p>Data MUST not be altered, removed, or deleted, just marked as altered, removed, or deleted.</p> <p>Audit trail MUST be printable:</p> <p>a) Separately from the recorded information for each patient b) Cannot contain references that are meaningless outside of the EMR Offering context</p> <p>Refer to the “CPSO Policies - Medical Records” in the Related Documents section for audit requirements.</p>		
PS02.02	<p>MUST have an audit trail for all add/change/delete operations on all EMR (non-medical record) data, including permission metadata.</p> <p>Data MUST not be altered, removed, or deleted, just marked as altered, removed, or deleted.</p>	<p>Non-medical data includes practice management data (i.e., appointments, billing) and EMR configuration data that deals specifically with customizable behaviour of the EMR Offering.</p> <p>Updated information MUST retain original data entry as well.</p>	M	P
PS02.03	<p>MUST NOT allow for the capability to disable the audit trail. This applies to medical and non-medical records within the EMR Offering</p>	<p>This functionality is mandatory per CPSO regulations (see CPSO Medical Records Policy).</p>	M	P
PS02.04	<p>Each record in the EMR Offering will include a date/time stamp and user ID for the update of that record</p>	<p>Can be visible either on the chart or through an audit trail</p>	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS02.05	Audits and logs all logins, successful and failed, at the EMR server	<p>The log MUST include:</p> <ul style="list-style-type: none"> a) Timestamp b) EMR user ID/application ID c) Originating IP address d) Port accessed or computer name <p>Both local and remote logins MUST be auditable.</p>	M	P
PS02.06	Audits and logs traffic that indicates unauthorized activity encountered at the EMR server	<p>The log MUST include:</p> <ul style="list-style-type: none"> a) Timestamp b) User ID/application ID c) Originating IP address d) Port accessed or computer name <p>Anonymous access for services installed and running on the server (e.g., FTP, Telnet, Web) is not allowed.</p> <p>If the EMR Offering does not require any additional services, i.e., the services are disabled, this requirement is then met.</p>	M	P
PS02.07	Audits and logs access to components of the medical record from outside the EMR Offering	<p>Including:</p> <ul style="list-style-type: none"> a) External ODBC connections used to execute SQL queries b) EMR data stored external to the database such as attachments c) All data files used to meet other EMR local requirements (e.g., reporting requirements) <p>The log MUST include timestamp, user ID/application ID and database operation.</p>	O	P
PS02.08	MUST synchronize the system time with a Network Time Protocol (NTP) server	System time MUST be synchronized with a trusted source to maintain audit trail integrity.	M	P

2.1.3 Privacy Requirements

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS03.01	The EMR Offering MUST comply with all Applicable Laws and regulations now or hereafter in force relating to privacy and the protection of personal information, including personal health information and enable health information custodians to comply with the requirements set out therein		M	P

2.1.4 Security Requirements

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS04.01	The EMR vendor MUST have an application-level Privacy Impact Assessment (PIA), and Threat and Risk Assessment (TRA) completed on the EMR Offering by an Information Security Professional with the appropriate credentials (e.g., CISSP: Certified Information Systems Security Professional).	The focus of the PIA and TRA is on the EMR Offering as a Commercial off-the-shelf (COTS) software and should take into account typical deployment scenarios but does not need to be completed for every installation at a clinic.	M	P
PS04.02	The EMR vendor MUST perform all TRAs in accordance with industry-accepted standards such as Harmonized Threat and Risk Assessment Methodology (HTRA) published by the Communications Security Establishment Canada (CSEC).		M	P

2.2 EMR Hosting

The following requirements in this section apply only to Hosted EMR Offerings and do not apply to Local EMR Offerings.

2.2.1 Threat Risk Management

OMD #	REQUIREMENT	M/O	STATUS
PS05.01	The EMR vendor MUST have a Privacy Impact Assessment (PIA) and a Threat and Risk Assessment (TRA) completed on the hosted EMR Offering by an Information Security Professional with the appropriate credentials (e.g., CISSP: Certified Information Systems Security Professional).	M	P
PS05.02	The EMR vendor MUST perform all TRAs in accordance with the industry-accepted standards such as Harmonized Threat and Risk Assessment Methodology (HTRA) published by the Communications Security Establishment Canada (CSEC).	M	P
PS05.03	The EMR vendor shall make executive summaries (results) of TRAs and relevant risk treatment plans available on request from subscribers and OntarioMD within three business days upon approval of the TRA by the EMR vendor's Chief Information Officer (CIO).	M	P
PS05.04	The EMR vendor shall maintain: <ul style="list-style-type: none"> a) An asset listing that contains valuation and classification ratings for the hosted EMR Offering b) A risk listing that contains threat and vulnerability ratings for the hosted EMR Offering 	M	P
PS05.05	The EMR vendor MUST treat all completed or partially completed TRAs and supporting documentation in accordance with the protection requirements for information classified as Confidential.	M	P
PS05.06	The EMR vendor MUST have a TRA or delta TRA performed on the hosted EMR Offering under the following conditions: <ul style="list-style-type: none"> a) Prior to a significant modification to existing back-end architecture or functionality b) Prior to significant changes to existing front-end technical design or functionality c) Prior to significant changes to operational support models, tools, processes, or parties d) Prior to significant changes to existing policies or procedures e) Prior to a change of electronic service provider f) Prior to changes to applicable agreements that could be expected to impact the privacy of individuals or the security of their PHI g) Prior to legislative changes to the Personal Health Information Protection Act (PHIPA) that could be expected to impact the privacy of individuals or the security of their PHI 	M	P

OMD #	REQUIREMENT	M/O	STATUS
	h) On discovery of a vulnerability that resulted in, or could have resulted in, an information security incident as deemed necessary by OntarioMD i) At a minimum, every two years if none of the above has initiated a comprehensive TRA		
PS05.07	The EMR vendor MUST document a risk treatment option for all risks identified through the TRA process. Risk treatment options may include one or more of the following: a) Applying additional information security controls to further reduce the risk b) Accepting the risk c) Avoiding the risk by not allowing actions that would cause the risk to occur	M	P
PS05.08	Where the EMR vendor chooses as the risk treatment option to apply additional information security controls, these controls MUST be implemented to meet the requirements identified in the TRA.	M	P
PS05.09	The EMR vendor MUST document and monitor all their accepted risks in a risk register with identified owners, action plans (risk treatment option details), and status. Risks should be reviewed quarterly, and risk treatment options updated if required.	M	P
PS05.10	The EMR vendor MUST submit TRAs approved by the EMR vendor's CIO to OntarioMD upon request.	M	P