Privacy and Security

Requirements

November 3, 2023

Document Version and Status: 2.0 – Final

Table of Contents

1. INTRODUCTION 3

1.1 OVERVIEW 3
1.2 VERSION HISTORY 3
1.3 SCOPE 4
1.4 ASSUMPTIONS 4
1.5 RELATED DOCUMENTS, REFERENCES AND SOURCES 4

2. REQUIREMENTS 5

2.1 DATA AND SYSTEM ACCESS MANAGEMENT 6
2.2 AUDITING AND LOGGING 9
2.3 PRIVACY 12
2.4 THREAT AND RISK MANAGEMENT 14
2.5 PENETRATION TESTS 18
2.6 VULNERABILITY ASSESSMENT 20
2.7 SECURITY PROCESSES AND CONTROLS AUDIT 22

1. INTRODUCTION

1.1 Overview

This document defines functional and non-functional requirements and provides guidance on privacy and security requirements applicable to an EMR Offering in a clinical healthcare setting. The purpose of these requirements is to uphold and maintain the security and privacy of patient health information used or stored by these systems and services. The intended audience of this document includes business and technical implementers of an EMR Offering.

1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2020-09-10	a) Initial release i) Moved requirements originally from Primary Care Baseline Specification: 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 1. PS05.XX from HST08.XX
2.0	2023-10-16	a) General updates and re-organization of sections and requirements within the document to be inclusive of both Hosted and Local EMR Offerings. This document no longer maintains separate sections of requirements pertaining to Local vs. Hosted Offerings. b) Inclusion of checklists as guidance for documents to include in PIA, TRA and penetration testing reports. c) Added PS03.02 through PS03.05 to align privacy requirements with security requirements. d) Updated PS04.01: Updated list of accepted credentials to perform a TRA e) Updated PS04.02: Expanded list of accepted TRA methodologies f) Updated PS04.03: Updated listing of content to include in a TRA report g) Added PS04.06: Separated requirement for validity period for a TRA h) Updated PS04.07: Updated for clarity of some of the change conditions i) Updated PS04.08: Changed evaluation of a risk treatment plan to follow national standards for vulnerability severity ratings j) Updated PS04.09: Elaborated on information to include in a risk register k) Added PS05.01 through PS05.04: Added a new section to cover requirements relating to penetration testing l) Retired PS05.05 (Protecting confidential information) m) Retired PS05.08 (Risk treatment option controls) n) Added PS06.01 through PS06.03: Added a new section to cover requirements relating to security process and controls audit

1.3 Scope

- The requirements in this document apply to Hosted and Local EMR Offerings unless otherwise stated.

1.4 Assumptions

- Readers have a general understanding of EMRs and their functionality.
- Readers have a general understanding of privacy and security regulations and policies within their respective business domains and jurisdictions.

1.5 Related Documents, References and Sources

NAME	VERSION	DATE
CPSO Policies - Medical Records Management (College of Physicians and Surgeons of Ontario, 2022) https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Medical-Records-Management	N/A	2022-06
Harmonized Threat and Risk Assessment Methodology (Government of Canada, 2022) https://cyber.gc.ca/en/tools-services/harmonized-tra-methodology	N/A	2022-05-15
NIST SP 800-30 Guide for Conducting Risk Assessments (National Institute of Standards and Technology, 2021) https://www.nist.gov/privacy-framework/nist-sp-800-30	Revision 1	2023-04-23
Personal Health Information Protection Act, 2004 (King's Printer for Ontario, 2023) https://www.ontario.ca/laws/statute/04p03	N/A	2023-05-18
Vulnerability Metrics (National Institute of Standards and Technology (NIST), n.d.) https://nvd.nist.gov/vuln-metrics/cvss#	N/A	N/A

2. REQUIREMENTS

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

Support:

M = Mandatory. EMR Offerings certified for this specification MUST support this requirement.
O = Optional. Vendors MAY choose to support this requirement in their certified EMR Offering.

Status:

N = New requirement for this Specification version.
P = Previous requirement.
U = Updated requirement from the previous Specification version.
R = Retired requirement from the previous Specification version.

OMD #:

A unique identifier that identifies each requirement within OMD's Specification Library.

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 Data and System Access Management

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.01	The user MUST enter a password to access EMR Offering functions. The EMR Offering MUST store passwords in an encrypted format.	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	The EMR Offering MUST support complex passwords.	Passwords MUST include: a) Mixed case passwords b) Passwords of a minimum of eight characters c) Alphanumeric characters d) Special characters	M	P
PS01.03	The EMR Offering MUST have password management capabilities that can be deployed based on the user's discretion.	Password management capabilities include: 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 This applies to all passwords used within the EMR Offering, including the operating system and all applications.	M	P
PS01.04	The EMR Offering MUST be able to share patient data among authorized clinicians who access the same database.	MUST maintain proper clinician 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	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		that role. Multiple roles can be assigned to the user.		
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, 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 user	The user cannot use certain screens or capabilities of the EMR Offering.	M	P
PS01.09	There are access controls to data based on the user	The user cannot access certain data, even when the user can access a function that uses the data. It gives control over what the 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 content can be customized for different roles.	O	P
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	The EMR Offering MUST ensure the encryption of passwords and sensitive data.	The EMR Offering MUST ensure the encryption of: a) passwords transmitted over a wide area network (WAN) b) data that is transported across private or public networks c) data stored offline (e.g., backups, archives)	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.13	Provides the ability for multiple users to access the EMR Offering concurrently	Single-user access to EMR Offerings is not accepted.	M	P
PS01.14	Provides the ability for concurrent 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 users from simultaneously attempting to update a record with resultant loss of data.	M	P
PS01.16	Provides a way to quickly "lock" a user's workstation if left unattended	The following rules MUST apply: a) The 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) Data MUST not be accessible Acceptable solutions are: a) User-initiated lock (e.g., hotkey); and b) Screen lock with a timeout period	M	P
PS01.17	Ensures security when the user is logged on at multiple workstations	MUST be able to log on to the EMR Offering through a second workstation with the same user credentials without logging out of the first workstation.	M	P
PS01.18	Ensures security when several 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 user credentials without logging out the first user. The second user cannot see the first user's data and vice versa. If the MR Offering uses operating system features (e.g., user profile	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		switching) to meet this requirement, then a version of the OS that provides this feature MUST be included as part of the EMR Offering.		
PS01.19	Supports secure remote access	MUST be able to use all EMR functions when connected remotely. A VPN or equivalent secure connection MUST be supported for remote connections (e.g., for remote access from home).	M	U

2.2 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 Offering MUST be captured in the audit trail. The audit trail MUST: a) capture the date and time of the activity b) capture the User who accessed the data c) capture any changes in the recorded information d) preserve the original content of the recorded information when changed or updated Data MUST not be altered, removed, or deleted, just marked as altered, removed, or deleted. The audit trail MUST be printable: a) separately from the recorded information for each patient b) cannot contain references that are meaningless outside of the EMR Offering context	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Refer to the "CPSO Policies - Medical Records Management" in the Related Documents section for audit requirements.		
PS02.02	The EMR Offering MUST have an audit trail for all add/change/delete operations on all EMR (non-medical record) data, including permission metadata. Data MUST not be altered, removed, or deleted, just marked as altered, removed or deleted.	Non-medical data includes practice management data (i.e., appointments, billing) and EMR configuration data that deals specifically with any customizable behaviour of the EMR Offering. Updated information MUST retain original data entry as well.	M	P
PS02.03	The EMR Offering MUST NOT allow for the capability to disable the audit trail. This applies to medical and non-medical records within the EMR Offering.	This functionality is mandatory per CPSO regulations (see CPSO Medical Records Policy).	M	P
PS02.04	Each record in the EMR Offering will include a date and time stamp and user ID for the update of that record.	Can be visible either on the chart or through an audit trail	M	P
PS02.05	Audits and logs all logins to the EMR Offering	The logs MUST include: a) Timestamp b) User ID/application ID c) Originating IP address d) Port accessed or computer name Audits MUST include both successful and failed login attempts. Both local and remote logins MUST be auditable.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS02.06	Audits and logs traffic that indicates unauthorized activity encountered by the EMR Offering	The logs MUST include: a) Timestamp b) User ID/application ID c) Originating IP address d) Port accessed or computer name Anonymous access for services installed and running on the server (e.g., FTP, Telnet, Web) is not allowed. If the EMR Offering does not require any additional services, i.e., the services are disabled, this requirement is then met.	M	P
PS02.07	Audits and logs access to components of the medical record from outside the EMR Offering	Including: 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 requirements (e.g., reporting requirements) The log MUST include a timestamp, user ID/application ID and database operation.	O	P
PS02.08	The EMR Offering MUST maintain accurate system time.	The EMR Offering's date and time MUST be regularly synchronized with a trusted and precise time source to maintain audit trail integrity.	M	U

2.3 Privacy

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
PS03.02	The vendor MUST have a Privacy Impact Assessment (PIA) completed on the EMR Offering by an Information Privacy Professional.	The PIA MUST be conducted by an Information Privacy Professional with any of the following credentials in good standing: a) Certified Information Privacy Professional/Canada (CIPP/C) b) Certified Information Privacy Manager (CIPM) The vendor MUST provide supporting documents for the PIA upon request. At a minimum, a PIA MUST be conducted every two years.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS03.03	The vendor MUST submit the PIA report and the privacy risk treatment plan.	All of the following information MUST be submitted. a) PIA report b) Privacy risk treatment plan c) Information identified in the PIA checklist These documents along with any additional supporting documents identified in the PIA checklist MUST be approved by the vendor's Chief Security Officer, or by a representative holding an equivalent role. These documents MUST be provided to OMD within three business days upon request. Refer to the PIA checklist included in this specification for guidance on information to include in the PIA report.	M	N
PS03.04	The vendor MUST have a PIA performed on changes to the EMR Offering under specific conditions.	A PIA MUST be performed when any of the following conditions occur: a) Prior to changes to applicable agreements that could be expected to impact the privacy of individuals or the security of their Personal Health Information (PHI) b) 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 c) On discovery of a vulnerability that resulted in, or could have resulted in, an information privacy incident, as deemed necessary by the vendor and/or OMD.	M	N
PS03.05	The vendor MUST document a privacy risk treatment plan.	OMD may assess the privacy risk treatment plan to ensure that it accurately identifies and addresses all major risks.	M	N

2.4 Threat and Risk Management

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS04.01	The vendor MUST have a Threat and Risk Assessment (TRA) conducted on the EMR Offering by an independent third-party Information Security Professional with the appropriate credentials.	The TRA MUST be conducted by an Information Security Professional with any one of the following credentials: a) Certified Information Systems Security Professional (CISSP) b) Certified Information Security Manager (CISM) c) Certified Information Systems Auditor (CISA) d) Other credentials may be accepted upon review and consultation with OMD prior to conducting the TRA. The TRA MUST be conducted by an independent third-party Information Security Professional's who's credentials can be verified.	M	U
PS04.02	The TRA MUST be completed in accordance with an accepted methodology.	The TRA MUST be completed in accordance with one of the following accepted methodologies. a) Harmonized Threat and Risk Assessment Methodology (HTRA) b) National Institute of Standards and Technology (NIST) SP 800-30	M	U
PS04.03	The vendor MUST submit the TRA report and relevant security risk treatment plan(s).	All of the following information MUST be submitted with the TRA report: a) Security risk treatment plan(s) b) Information identified in the TRA checklist These documents along with any additional supporting documents identified in the TRA checklist MUST be approved by the vendor's Chief Security Officer, or by a representative holding an equivalent role. These documents MUST be provided to OMD within three business days upon request. The TRA report MUST include all the following information:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) Scope d) Existing safeguards e) Identified findings f) Vulnerabilities g) Risk calculations h) Residual risk i) Mitigations j) Time plan for mitigations Any sensitive or proprietary content or information that can lead to asset identification, or other information disclosure (e.g., IP address, embedded URLs, etc.) can be redacted (i.e., concealed, removed or deleted). Refer to the TRA checklist included in this specification for guidance on information to include in the TRA report.		
PS04.04	The vendor MUST maintain an asset listing for the EMR Offering.	The asset listing for the EMR Offering MUST contain: a) valuation to assess the impact in case of damage or loss of use, and b) classification ratings. **Note**: Assets are defined by all systems, services and integrations required to deliver the EMR Offering service.	M	U
PS04.05	The vendor MUST maintain a risk listing for the EMR Offering.	The risk listing MUST include threat and vulnerability ratings.	M	P
PS04.06	The vendor MUST have a TRA performed on the full scope of the EMR Offering every two years.	A refreshed TRA encompassing the full scope of the current EMR Offering MUST be performed every two years from the date of the previous TRA.	M	N
PS04.07	The vendor MUST have a TRA performed on changes to the EMR Offering under specific conditions.	The TRA MUST be performed under any of the following conditions: a) Prior to the release of a significant modification to existing back-end architecture or functionality b) Prior to the release of significant changes to existing front-end technical design or functionality	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) Prior to the release of significant changes to operational support models, tools, processes, or parties d) Prior to the release of 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 Personal Health Information (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 h) On discovery of a vulnerability that resulted in, or could have resulted in, an information security incident as deemed necessary by the vendor or OMD.		
PS04.08	The vendor MUST document a security risk treatment plan for all risks identified as part of the TRA process.	Vulnerability severity ratings MUST align with or map to the Common Vulnerability Scoring System (CVSS) v3.0 or higher, as defined by NIST. Refer to the "Vulnerability Metrics". Known or identified vulnerabilities MUST be remediated, mitigated or avoided, transferred or accepted within a defined and prudent timeline based on severity level. OMD maintains the discretion to review the security risk treatment plan to ensure that it accurately identifies and addresses all risks.	M	U
PS04.09	The vendor MUST document and monitor all their accepted risks in a risk register.	The risk register MUST identify all the following information. a) Responsible risk owner(s) b) Action plans (risk treatment option details), if applicable c) Risk status	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Risks SHOULD be reviewed at least quarterly and risk treatment options updated if required.		

2.5 Penetration Tests

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS05.01	The vendor MUST perform penetration tests on the EMR Offering, at a minimum, every 12 months on all customer-facing or Internet-facing applications.	Penetration tests MUST be conducted by an independent third-party Information Security Professional with at least one of the following credentials in good standing. a) Certified Ethical Hacker (CEH) b) Offensive Security Certified Professional (OSCP) c) GIAC Penetration Tester (GPEN) The Information Security Professional conducting penetration testing MUST be from an external organization specializing in information security reviews, and who's credentials can be verified. **Note**: The penetration testing applies to both Local and Hosted EMR Offerings. The following scope applies: • **Local Offerings**: The application and reference architecture, which is the documented architectural design of how the EMR Offering was intended to be deployed and used • **Hosted Offerings**: The EMR application and the hosting environment	M	N
PS05.02	The vendor MUST have a penetration test performed on changes to the EMR Offering under specific conditions.	A penetration test MUST be performed on the changes to the EMR Offering when any of the following conditions occur. a) Prior to the release of a significant modification to existing back-end architecture or functionality b) Prior to the release of significant changes to existing front-end technical design or functionality c) Prior to the release of a change of service provider d) Prior to changes to applicable agreements that could be expected to impact the privacy of individuals or the security of Personal Health Information (PHI) e) On discovery of a vulnerability that resulted in an information security incident.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS05.03	The vendor MUST submit a report of the penetration tests performed.	At a minimum, the report MUST identify all of the following information. a) Scope of the tests performed b) Dates of the penetration testing c) Testing methodology d) Target systems details e) Identified vulnerability details including severity classification f) Exploitation details g) Risk assessment h) Penetration testing findings and recommendations i) Remediation plan and evidence of remediation steps taken j) Existing safeguards k) Residual risk The report MUST be provided to OMD once every 12 months. OMD may request an ad-hoc report upon request. These documents, along with any additional supporting documents identified in the penetration test checklist, MUST be approved by the vendor's Chief Security Officer, or by a representative holding an equivalent role. Any sensitive or proprietary content or information that can lead to asset identification, or other information disclosure (e.g., IP address, embedded URLs, etc.) can be redacted (i.e., concealed, removed or deleted). Refer to the penetration testing checklist included in this specification for guidance on information to include in the penetration testing report.	M	N
PS05.04	The vendor MUST document a security risk treatment plan for all vulnerabilities identified.	Vulnerability severity ratings MUST align with or map to the CVSS v3.0 or higher, as defined by NIST. Refer to the "Vulnerability Metrics". Known or identified vulnerabilities MUST be remediated or mitigated within a defined and prudent timeline based on severity level.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		OMD maintains the discretion to review the security risk treatment plan to ensure that it accurately identifies and addresses all risks.		

2.6 Vulnerability Assessment

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS06.01	The vendor MUST perform vulnerability and configuration scans, at a minimum, every three months on the EMR Offering.	Vulnerability and configuration scans MAY be conducted by an internal Information Security Professional. At a minimum, the vulnerability assessment MUST include the following information. a) Scope of the scans performed b) Identified vulnerability details including severity classification c) Either the date of the scans performed or the frequency of scheduled scans d) Remediation plan and evidence of remediation steps taken **Note**: Vulnerability assessments apply to both Local and Hosted EMR Offerings. The following scope applies: • **Local Offerings**: The application and reference architecture, which is the documented architectural design of how the EMR Offering was intended to be deployed and used • **Hosted Offerings**: The EMR application and the hosting environment	M	N
PS06.02	The vendor MUST submit a report of the vulnerability and configuration scans performed.	The report MUST identify all of the following information. a) Scope of the scans performed b) Identified vulnerability details including severity classification.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) Either the date of the scans performed or the frequency of scheduled scans d) Remediation plan and evidence of remediation steps taken The report MUST be provided to OMD every two years. OMD may request an ad-hoc report upon request. **Note**: Sensitive information (e.g., specific vulnerabilities, IP addresses) is not required and should not be included in the submitted report.		
PS06.03	The vendor MUST document a security risk treatment plan for all vulnerabilities identified by a vulnerability assessment, to be provided upon request.	Vulnerability severity ratings MUST align with or map to the CVSS v3.0 or higher, as defined by NIST. Refer to the "Vulnerability Metrics". Known or identified vulnerabilities MUST be remediated or mitigated within a defined and prudent timeline based on severity level. OMD maintains the discretion to review the security risk treatment plan to ensure that it accurately identifies and addresses all risks.	M	N

2.7 Security Processes and Controls Audit

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS07.01	The vendor MUST regularly conduct a security audit of its current processes and controls that support data security and privacy.	One of the following reports or certifications MUST be maintained in good standing: a) SOC 2 Type 2 audit report b) ISO/IEC 27001 certification At a minimum, the security control audit MUST include all the following: a) EMR Offering development environment b) Personnel c) Data centres d) Company processes and policies The security process and controls audit covering the above scope MUST be refreshed at least every 12 months. Substantiation of the SOC 2 Report or ISO/IEC 27001 Certificate of Registration MUST be provided to OMD upon request.	M	N