

Privacy and Security

Requirements

September 11, 2026

Document Version and Status: 2.2 – DFC



Table of Contents

1. INTRODUCTION	3
1.1 OVERVIEW.....	3
1.2 VERSION HISTORY	3
1.3 SCOPE	5
1.4 ASSUMPTIONS.....	6
1.5 RELATED DOCUMENTS, REFERENCES AND SOURCES	6
2. REQUIREMENTS	8
2.1 DATA AND SYSTEM ACCESS MANAGEMENT	9
2.2 AUDITING AND LOGGING	18
2.3 PRIVACY	22
2.4 THREAT AND RISK MANAGEMENT	24
2.5 SECURITY PROCESSES AND CONTROLS AUDIT.....	28
2.6 VULNERABILITY SCANS	33
3. APPENDICES	34
3.1 APPENDIX A: GLOSSARY	34
3.2 APPENDIX B: MINIMUM PASSWORD REQUIREMENTS	36
3.3 APPENDIX C: APPROVED CRYPTOGRAPHIC ALGORITHMS.....	38

1. INTRODUCTION

1.1 Overview

This document defines functional and non-functional requirements and provides guidance on privacy and security controls applicable to an EMR Offering in a clinical healthcare setting.

These requirements are intended to support the protection of patient health information that is created, accessed, stored, transmitted, or processed by EMR systems and related services.

The intended audience for this document includes business, technical, and operational stakeholders responsible for the design, implementation, operation, and support of an EMR Offering.

1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
2.2	2026-09-11	a) Updated PS01.01 – Added Reference to ISO 27001. b) Updated PS01.02 – Updated the requirement to align with industry best practices for digital identity guidelines. c) Updated PS01.03 – Guidelines updated to reflect latest guidance from NIST SP800-63B Digital Identity Guidelines. d) Updated PS01.06 – Guidelines updated to align with industry best practices for digital identity guidelines. e) Updated PS01.07 – Guidelines updated to reflect latest guidance from NIST SP800-63B Digital Identity Guidelines. f) Updated PS01.08 – Added additional clarifying details. g) Updated PS01.09 – New Requirement added to ensure both local and hosted EMR Offering support the ability to disable accounts based on inactivity. h) Updated PS01.10 – Added additional clarifying details. i) Updated PS01.12 – Guidelines updated to reflect latest changes to Appendix C: Approved Cryptographic Algorithms in accordance with industry best practices. j) Updated PS01.20 – Updated that Remote connections must support MFA to reflect latest changes to Appendix C: Approved Cryptographic Algorithms. k) Updated PS01.21 – Added requirement for vendors to implement MFA and support Authentication Level Assurance Level 2 (AAL2) or higher in accordance with industry best practices. l) Added PS01.23 – Added requirement ‘Breaking the Glass’ temporary override capability. m) Added PS01.24 – Added dual-control workflow to complement PS01.21. n) Added PS01.25 – Added logging requirement to complement PS01.21. o) Added PS01.26 – Added optional data classification requirement. p) Added PS01.27 – Added optional requirement for vendors to enable policy-based access controls in support for Zero Trust Architecture. q) Updated PS02.01 and PS02.02 – The two complementary requirements have been merged.

VERSION	REVISION DATE	REVISION NOTES
		r) Updated PS02.04 – Guidelines updated to reflect latest industry best practices. s) Updated PS02.05 – Guidelines updated to align with industry best practices for digital identity guidelines. t) Updated PS02.06 – Guidelines updated to align with industry best practices for digital identity guidelines. u) Updated PS03.01 – Updated to add additional clarifying guidelines. v) Updated PS03.02 – Guidelines updated to Chief Privacy Officer for PIA accountability. w) Updated PS03.04 – Updated requirement to reflect the need for a risk mitigation plan rather than a risk treatment plan. x) Updated PS04.06 – Guidelines updated to clarify asset inventory requirements. y) Updated PS04.07 – Guidelines updated to reflect the current version of CVSS v3.1. z) Updated PS04.08 – Updated requirement to reflect the need for a risk mitigation plan rather than a risk treatment plan. aa) Updated PS05.01 and PS05.02 – requirement has been broken down into 5 (five) distinct requirements for readability: a) PS05.01 – Security Controls Audit Requirements b) PS05.02 – Audit Scope c) PS05.03 – Deployment model considerations (Hosted vs Local) d) PS05.04 – Certification/Audit report maintenance e) PS05.05 – Certification/Audit reporting bb) Added PS05.07 – Added Penetration Test Requirements cc) Added PS05.08 – Added Penetration Test Credentials dd) Added PS05.09 – Added Penetration Test Scope ee) Added PS05.10 – Added Security Treatment Plan and Remediation Expectations ff) Added 2.6 Vulnerability Scans Requirements: • PS06.01 – VA Scanning Requirements • PS06.02 – VA Scanning Scope • PS06.03 – VA Scan Reporting and Risk Mitigation Plan gg) Updated Appendix B: Minimum Password Requirements in alignment with industry best practices. hh) Updated Appendix C: Approved Cryptographic Algorithms in alignment with industry best practices for digital identity guidelines. ii) Added hosted and local deployment applicability guidance across Privacy and Security sections. jj) New Requirement PS05.01 – Added deployment model considerations for security controls audit scope. kk) New Requirement PS05.08 – Added requirement for penetration testing on changes to the EMR Offering. ll) New Requirement PS05.09 – Added penetration testing frequency and credential requirements. mm) New Requirement PS05.10 – Added penetration test reporting requirements. nn) New Requirement PS05.11 – Added security risk treatment plan requirement for penetration testing findings. oo) New Requirement PS06.01 – Added deployment model considerations for vulnerability and configuration scanning controls.

VERSION	REVISION DATE	REVISION NOTES
		pp) New Requirement PS06.02 – Added vulnerability and configuration scanning requirements. qq) New Requirement PS06.03 – Added vulnerability and configuration scan reporting requirements. rr) New Requirement PS02.07 – Added human-readable audit log requirement and guidelines. ss) The following requirements were moved from Primary Care Baseline to Privacy and Security: • PS01.28 from PC14.04 • PS01.29 from PC14.05 • PS01.30 from PC14.06 • PS01.31 from PC14.07 • PS01.32 from PC14.08 tt) Updated Requirement IDs: • PS01.10 from PS01.09 • PS01.11 from PS01.10 • PS01.12 from PS01.11 • PS01.13 from PS01.12 • PS01.14 from PS01.13 • PS01.15 from PS01.14 • PS01.16 from PS01.15 • PS01.17 from PS01.16 • PS01.18 from PS01.17 • PS01.19 from PS01.18 • PS01.20 from PS01.19 • PS02.01 from PS02.01 and PS02.02 • PS02.02 from PS02.03 • PS02.03 from PS02.04 • PS02.04 from PS02.05 • PS02.05 from PS02.06 • PS02.06 from PS02.08 • PS05.01–PS05.04 from PS05.01 • PS05.05 from PS05.02

1.3 Scope

- The requirements in this document apply to both Local and Hosted EMR Offerings unless explicitly stated otherwise.
- The scope includes the EMR Offering, supporting services, operational processes, personnel, and technical environments used to collect, use, disclose, store, transmit, retain, protect, monitor, manage, or dispose of information associated with the EMR Offering.
- The requirements apply to the EMR Vendor, and any agents, suppliers, subcontractors, or electronic service providers involved in the delivery, operation, support, or management of the EMR Offering.

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

CATEGORY	NAME	VERSION	DATE
Clinical / Regulatory	CPSO Policies – Medical Records Management (College of Physicians and Surgeons of Ontario) https://www.cpso.on.ca/Physicians/Policies-Guidance/Policies/Medical-Records-Management	N/A	2022-06
Regulatory	Personal Health Information Protection Act, 2004 (PHIPA) https://www.ontario.ca/laws/statute/04p03	N/A	2024-06-28
Regulatory / Privacy	Privacy Impact Assessment Guidelines (Information and Privacy Commissioner of Ontario) https://www.ipc.on.ca/wp-content/uploads/resources/phipa_pia-e.pdf	N/A	Current
Canadian Guidance	Harmonized Threat and Risk Assessment (TRA) Methodology (Canadian Centre for Cyber Security) https://cyber.gc.ca/en/tools-services/harmonized-tra-methodology	N/A	2022-05-15
Canadian Guidance	Protecting Your Organization from Software Supply Chain Threats – ITSM.10.071 (Canadian Centre for Cyber Security) https://www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071	Revision 1	2023-02-08
NIST SP 800 Series	NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	Revision 5	2020
NIST SP 800 Series	NIST SP 800-63B – Digital Identity Guidelines: Authentication and Authenticator Management https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf	Revision 4	2023
NIST SP 800 Series	NIST SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf	Revision 1	2012
NIST SP 800 Series	NIST SP 800-60 Vol. 1 Rev. 1 – Guide for Mapping Types of Information and Information Systems to Security Categories https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf	Revision 1	2008

CATEGORY	NAME	VERSION	DATE
NIST SP 800 Series	NIST SP 800-92 – Guide to Computer Security Log Management https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf	N/A	2006
NIST SP 800 Series	NIST SP 800-38A – Recommendation for Block Cipher Modes of Operation https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf	N/A	2001
NIST SP 800 Series	NIST SP 800-38D – Galois/Counter Mode (GCM) and GMAC https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf	N/A	2007
NIST SP 800 Series	NIST SP 800-207 – Zero Trust Architecture https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf	N/A	2020
Industry Standard (NIST NVD)	Vulnerability Metrics (National Institute of Standards and Technology (NIST), 2024) https://nvd.nist.gov/vuln-metrics/cvss#	N/A	2024-06-27
ISO Standard	ISO/IEC 27001 – Information Security Management Systems https://www.iso.org/standard/27001	2022	2022
ISO Standard	ISO/IEC 27002 – Information Security Controls https://www.iso.org/standard/75652.html	2022	2022
ISO Standard	ISO/IEC 27701 – Privacy Information Management ISO/IEC 27701 https://www.iso.org/standard/71670.html	2019	2019

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 EMR Offering MUST store passwords in an encrypted format.	Passwords managed by the EMR Offering MUST be stored using secure one-way hashing mechanisms consistent with recognized industry standards e.g. ISO 27001. The EMR Offering MUST ensure that stored passwords cannot be retrieved or decrypted in plaintext form. Passwords managed by external systems (e.g., operating systems or identity providers) MUST rely on the security controls provided by those systems. For passkey implementations, the EMR Offering MUST comply with the current WebAuthn specification and applicable FIDO2 requirements, MUST securely store the public key and credential identifier, and MUST NOT receive or store the associated private key.	M	U
PS01.02	The EMR Offering MUST support strong password authentication consistent with industry security best practices.	The EMR vendor MUST implement password controls that support secure authentication practices, including: a) Support for passwords or passphrases with a minimum length of at least eight (8) characters with multi-factor authentication (MFA), and at least fifteen (15) characters where passwords are used as the sole authentication factor. b) Support long passphrases with a maximum length of at least 64 characters. c) Mechanisms to prevent the use of commonly used, weak, or compromised passwords. d) Secure storage of passwords using cryptographic hashing resistant to offline attacks. e) Protections against brute-force and credential-stuffing attacks, such as rate limiting, progressive delays, or account lockout thresholds. Detailed password composition, lifecycle, and account protection requirements are defined in Appendix B: Minimum Password Requirements.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.03	The EMR Offering MUST have password management capabilities that can be deployed based on the user's discretion.	The EMR Offering MUST provide configurable password management controls aligned with recognized security standards. These Controls MUST include: a) The ability for authorized administrators to configure limits on consecutive failed authentication attempts to protect against online guessing attacks. b) The implementation of rate-limiting or throttling mechanisms to restrict repeated failed login attempts. c) Administrative capabilities to reset or revoke user passwords where required. d) Application of these controls to authentication mechanisms within the EMR Offering, including application services and administrative interfaces under the vendor's control. The EMR Offering MAY provide the ability for authorized administrators to configure time parameters for password expiry.	M	U
PS01.04	The EMR Offering MUST be able to share patient data among authorized clinicians who access the same database.	The EMR Offering MUST maintain proper clinician identification. Patient data MUST only be shared if permitted by practice rules.	M	P
PS01.05	The EMR Offering MUST provide the capability to create roles.	The EMR Offering MUST support role-based access control with the ability to create and manage roles with configurable permissions. These controls MUST include: a) The ability to create new roles with customized permissions. b) The ability to modify role permissions, where changes are applied consistently to all users assigned to that role. c) The ability to assign multiple roles to a single user. The EMR Offering MUST NOT be limited to pre-defined roles only.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.06	The EMR Offering MUST implement role-based access control mechanisms.	The EMR Offering MUST implement role-based access control mechanisms: a) The ability to assign permissions and restrictions to specific roles, determining access to screens, system functions, and data within the EMR Offering. b) The ability to assign roles to individual users or groups of users. c) Administrative capabilities to define, modify, and manage roles and associated permissions. d) Enforcement of least-privilege access, ensuring users only have access to the functions required for their role. Example: The EMR Offering should ensure that sensitive administrative functions (e.g., record merge functions) can be assigned only to specific users, roles, or groups with appropriate authorization.	M	U
PS01.07	The EMR Offering MUST enforce controls that restrict access to data based on assigned user roles.	The EMR Offering MUST ensure that authorization controls restrict access to information in accordance with assigned user roles. These controls MUST include: a) The ability to restrict access to specific data elements, records, or datasets, even where a user role is permitted to access the associated system function. b) Enforcement of data-level access restrictions at the logical or record level within the EMR Offering. c) Administrative capabilities to configure and manage role permissions governing data access. d) Enforcement of least-privilege access, ensuring users can only view or modify data necessary for their assigned role. Example: A role may have permission to access a function (e.g., patient record search) but may also be restricted from viewing or modifying certain data elements or records within that function.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.08	The EMR Offering MUST enforce controls that restrict access to system functions based on individual user permissions.	The EMR Offering MUST ensure that authorization controls restrict access to system functions based on individual user permissions. These controls MUST include: a) The ability to restrict access to specific screens, functions, or capabilities for individual users. b) Enforcement of user-specific access restrictions, independent of or in addition to role-based permissions. c) Administrative capabilities to configure and manage user-level permissions. d) Enforcement of least-privileged access, ensuring users can only access functions necessary for their assigned responsibilities.	M	U
PS01.09	The EMR Offering MUST support controls to disable accounts that have been inactive for a defined period.	Controls MUST ensure that: a) accounts are automatically or manually disabled after 180 days of inactivity b) users may be notified prior to suspension c) reactivation requires reauthorization	M	N
PS01.10	The EMR Offering MUST enforce controls that restrict access to data based on individual user permissions.	The EMR Offering MUST ensure that authorization controls restrict access to information based on individual user permissions. These controls MUST include: a) The ability to restrict access to specific data elements, records, or datasets for individual users. b) Enforcement of data-level access restrictions, even when the user has permission to access the associated system function. c) Administrative capabilities to define and manage user-specific data access permissions. d) Enforcement of least-privilege access, ensuring users can only view or modify data necessary for their authorized activities. Example: Users may perform functions such as scheduling appointments or billing services without being granted access to the patient's full clinical record.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.11	The EMR Offering MUST support role-based configuration of user interface views.	The EMR Offering MUST support the ability to configure and present different views of data based on assigned user roles. These controls MUST include: a) The ability to customize screen layout, organization, or displayed content for different roles. b) The ability to control visibility of specific data elements or sections within the user interface based on role. c) Administrative capabilities to configure and manage role-based view settings. d) Enforcement of role-based views in alignment with assigned permissions and access controls.	O	U
PS01.12	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	U
PS01.13	The EMR Offering MUST ensure the encryption of passwords and sensitive data.	The EMR Offering MUST ensure that encryption mechanisms protect passwords and sensitive data during transmission and storage in accordance with Appendix C: Approved Cryptographic Algorithms. These controls MUST include: a) Protection of passwords and credentials transmitted across networks using secure communication protocols. b) Encryption of sensitive data transmitted across private or public networks. c) Encryption or equivalent protection of sensitive data stored on end-user devices where the EMR Offering stores or caches such information locally e.g. data stored on mobile phones, tablets. d) Use of approved cryptographic algorithms and key lengths consistent with the organization's cryptography standards. e) Protection and management of encryption keys using mechanisms appropriate to the deployment model (e.g., hosted or local environments).	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.14	Provides the ability for multiple users to access the EMR Offering concurrently	Single-user access to EMR Offerings is not accepted.	M	U
PS01.15	Provides the ability for concurrent users to simultaneously view the same record	Refers to practice management information, as well as clinical information.	M	U
PS01.16	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	U
PS01.17	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 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 include: i. User-initiated lock (e.g., hotkey); and ii. Screen lock with a timeout period	M	U
PS01.18	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	U
PS01.19	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 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 Offering.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.20	The EMR Offering MUST ensure that users are able to securely access all EMR functions when connected remotely.	The EMR Offering MUST ensure that users are able to access all EMR functions when connected remotely. A VPN or equivalent secure remote access mechanism MUST be supported for remote connections (e.g., remote access from home) and MUST support multi-factor authentication (MFA). Remote access connections MUST be protected using encrypted communication protocols in accordance with Appendix C: Approved Cryptographic Algorithms.	M	U
PS01.21	The EMR vendor MUST implement and enforce Multifactor Authentication (MFA) for any account that accesses PHI or provides administration to the EMR offering.	The EMR Offering MUST implement MFA controls and support authentication mechanisms consistent with Authentication Assurance Level 2 (AAL2) or higher. These controls MUST include: a) All accounts with access to PHI b) Administrative or elevated privileges c) All remote access connections d) Access to any web-based portals or cloud-hosted components	M	N
PS01.22	The EMR Offering MUST enforce controls that restrict access to a specific patient record.	Access to the patient record by any user not assigned to the patient's active care team MUST be blocked by default. Note: if override is supported, then this requirement becomes mandatory.	O	N
PS01.23	The EMR Offering MUST provide a mechanism for a clinical user to temporarily override access control restrictions on a client's record in a clinical emergency. IE. Breaking the glass.	The following rules MUST apply when overriding a restricted client record: a) MUST only persist until logout b) MUST be required to enter a reason for the override c) MUST be limited only to clinical roles Note: if override is supported, then this requirement becomes mandatory.	O	N
PS01.24	The EMR Offering SHOULD support a dual-control workflow for all break glass access requests.	When breaking glass on a client record the EMR Offering SHOULD require approval from a second, authorized user.	O	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.25	The EMR Offering MUST log all client record overrides in the audit log.	The EMR Offering MUST record all break glass events to the audit log. The audit log MUST record the following: a) Name or user account who requested the override b) Location of the user account who requested the override (IP address) c) Name of the approver, user account and location of the user account who approved the override (IP address) d) Name of client record accessed e) Date/Time of the override f) Reason provided for the override g) What information was accessed at the time of override h) Any override attempts by non-clinical EMR users Note: if override is supported, then this requirement becomes mandatory.	O	N
PS01.26	The EMR Offering MUST provide the capability to classify and label information according to sensitivity and risk level.	The EMR Offering MUST support the classification of information to enable the application of appropriate privacy and security controls. Classification capabilities SHOULD include, as applicable: a) Assignment of data sensitivity or security categories to records, documents, or information objects. b) The ability to identify and apply enhanced access controls to sensitive or restricted information. c) Alignment with recognized information classification. d) Support for downstream security controls including access restriction, audit logging, consent management, and emergency override (“break-the-glass”) capabilities.	O	N
PS01.27	The EMR Offering MUST support policy-based access controls that allow authorization decisions based on user attributes, context, or system conditions.	The EMR Offering MUST support access control mechanisms that evaluate attributes and contextual factors when determining access to EMR functions or data. These controls MUST include: a) Authorization decisions based on user attributes (e.g., role, organization, credentials).	O	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) Consideration of contextual attributes, such as device type, location, or authentication strength. c) The ability to enforce dynamic access policies based on defined security conditions. d) Integration with enterprise identity or policy engines where applicable.		
PS01.28	The EMR Offering MUST provide a complete system (applications and data) backup and recovery process.	Based on Ontario Regulation 114/94, Section 20 (7). Back-up can be full or incremental, etc. Recovery can be to the last backup, point of failure, etc.	M	U
PS01.29	The EMR Offering SHOULD store the external documentation using a database solution.	Refer to the external documentation described in section 2.6 External Document Management A solution that stores documents in the file system (server or client) only does not satisfy the requirement.	O	U
PS01.30	The EMR Offering SHOULD encrypt patient data and clinical management data resident on server(s) with a strength of at least 128-bits.	A solution that only encrypts data as it is transmitted over the network does not satisfy the requirement.	O	U
PS01.31	The EMR Offering MUST harden the EMR server in preparation for server-level encryption.	Server hardening consists of creating a baseline for the security of the application server. Threats to Personal Health Information breaches via external access are greatly reduced by eliminating entry points and minimizing system software. Physical security is elevated when all application data and information is encrypted. This guideline does not apply to Hosted EMR Offerings. Refer to the "Server Hardening Checklist" in the Related Documents section.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS01.32	The EMR Offering MUST co-exist with an anti-malware solution on the same server without conflicts.	The EMR vendor MUST recommend to clients an anti-malware solution that does not negatively impact the EMR Offering. The recommended solution MUST coexist with the EMR Offering on the same server without creating any conflicts.	M	U

2.2 Auditing and Logging

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS02.01	The EMR Offering MUST maintain a comprehensive immutable audit trail for all medical record and non-medical EMR data.	The EMR Offering MUST maintain a complete application-level audit trail of medical records in accordance with CPSO Medical Records Management requirements. 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. Each patient record in the EMR Offering MUST have a distinct audit trail. The audit trail MUST capture all activity against medical records, including viewing, updating, and deleting information. 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 Medical record data MUST not be altered, removed, or deleted. Instead, records MUST be marked as altered, removed, or deleted while preserving the original content. The audit trail MUST be printable:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		a) separately from the recorded information for each patient b) without containing references that are meaningless outside of the EMR Offering context Refer to the CPSO Policies – Medical Records Management for detailed audit trail requirements.		
PS02.02	The EMR Offering MUST NOT allow for the capability to disable the audit trail. This applies to medical and non-medical records (including permission metadata) within the EMR Offering.	Audit trail functionality MUST be enforced at all times and MUST NOT be configurable for disablement by any user or administrator. This requirement aligns with CPSO Medical Records Management policy requirements for maintaining complete and accurate audit trails of medical records.	M	U
PS02.03	Each record in the EMR Offering will include a date and time stamp and user ID for the update of that record.	The EMR Offering MUST ensure that the date/time stamp and user identifier for each update are visible to authorized users: a) directly on the patient chart or record, and b) within the audit trail associated with the record. The audit trail MUST retain the complete history of updates made to the record.	M	U
PS02.04	Audit reports and logs include all authentication attempts to the EMR Offering.	The EMR Offering MUST record authentication events in audit logs. Logs MUST include: a) Timestamp of the authentication attempt b) User ID or application ID associated with the authentication attempt c) Originating IP address or device identifier d) Source system, port, or computer name, where available e) Outcome of the authentication attempt (successful or failed) Both local and remote authentication attempts MUST be auditable.	M	U
PS02.05	The EMR Offering MUST audit and log traffic that indicates unauthorized or suspicious activity encountered by the EMR Offering.	The logs MUST include: a) Timestamp b) User ID or application ID, where available c) Attempted user ID, where available	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		d) Originating IP address or device identifier e) Source system, port, or computer name f) Failure reason, where applicable g) The patient record or system object involved in the event, where applicable h) The type of action attempted or performed (e.g., view, create, update, delete, authentication failure) i) Identification of the information that was created, modified, or deleted, where applicable j) Anonymous access to services installed and running on the EMR Offering infrastructure MUST NOT be permitted, unless explicitly required and secured. Services that are not required for the operation of the EMR Offering MUST be disabled. Examples of services that may require secure configuration or disabling include file transfer services, remote access services, and web services.		
PS02.06	The EMR Offering MUST implement mechanisms to protect the integrity of audit logs and detect any alteration of log entries.	The EMR Offering MUST ensure that audit logs are protected from unauthorized modification, deletion, or tampering. Audit logging mechanisms MUST: a) Detect and record any attempt to alter or delete audit log entries b) Ensure that audit log integrity is preserved through tamper-evident or immutable logging mechanisms c) Capture database-level access and query activity, including queries executed directly against the database or through external interfaces d) Record sufficient information to determine what data was accessed, queried, or extracted Logging requirements apply to all mechanisms used to access EMR data, including: i. Database queries (e.g., SQL or equivalent query languages) ii. External database connections (e.g., ODBC, JDBC or similar interfaces) iii. Reporting or analytics tools iv. Administrative access mechanisms	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS02.07	The EMR Offering MUST present audit logs in a human-readable format that enables authorized users to easily identify all actions/activities anywhere in the EMR.	The intent of this requirement is to ensure that audit information is readily understandable and supports the review of changes made without requiring technical interpretation. Audit log information MUST be presented in a human-readable format to authorized EMR users, without EMR vendors involvement, that clearly defines the action(s) performed (access, create, modify, delete). The audit log MUST include: a) The information that was accessed, created, modified, or deleted; b) The previous and updated values for that information, where applicable; c) The identity of the individual who performed the action; d) The date and time stamp of the change. e) The patient record associated with the action (create, modify, or delete) f) Provide sufficient detail to allow a user to understand the action that occurred without requiring interpretation of system codes, database field names, or technical identifiers. Audit logs MUST NOT rely on internal codes, abbreviations, database field names, or technical descriptions to communicate the action. The audit log MUST be accessible within the EMR Offering's audit trail.	M	N

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.	The EMR vendor MUST ensure that the EMR Offering supports privacy and security controls that enable health information custodians to comply with the Personal Health Information Protection Act, 2004 (PHIPA). The EMR Offering MUST support custodians in meeting obligations related to: a) Establishing and maintaining documented information practices governing the collection, use, disclosure, retention, and disposal of personal health information. b) Implementing administrative, technical, and physical safeguards to protect personal health information from theft, loss, and unauthorized access, use, disclosure, copying, modification, or disposal. c) Ensuring that electronic systems used to collect, store, or transmit personal health information maintain the security and integrity of that information. d) Supporting custodians in ensuring that agents and service providers handle personal health information in accordance with the custodian's privacy obligations. e) Supporting requirements applicable to electronic service providers and network-based health information services.	M	U
PS03.02	The vendor MUST have a Privacy Impact Assessment (PIA) performed on the full scope of the EMR Offering by an Information Privacy Professional.	The PIA MUST align with PHIPA requirements and applicable guidance, including the Information and Privacy Commissioner of Ontario's Privacy Impact Assessment resources. The PIA MUST: a) Be conducted or led by a qualified privacy professional holding at least one of the following current certifications in active and good standing: • Certified Information Privacy Professional/Canada (CIPP/C) • Certified Information Privacy Manager (CIPM) b) Be conducted by an independent third party. c) Be completed at least once every two years. The EMR Vendor MUST provide supporting documentation and evidence of compliance upon request.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS03.03	The vendor MUST submit the PIA report.	All of the following information MUST be submitted. a) PIA report b) 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 Privacy Officer, or by a representative holding an equivalent role. The vendor MUST provide supporting documentation and substantiation upon request. Refer to the PIA checklist included in this specification for guidance on information to include in the PIA report.	M	U
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	P
PS03.05	The vendor MUST document a privacy risk mitigation plan.	OMD may request the privacy risk mitigation plan to ensure that it accurately identifies and addresses all major risks.	M	P

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 whose credentials can be verified.	M	P
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 Refer to the TRA checklist included in this specification for guidance when conducting an HTRA report.	M	P
PS04.03	The vendor MUST have a TRA performed on the full scope of the EMR Offering every two years by an independent third-party Information Security Professional.	The refreshed TRA encompassing the full scope of the current EMR Offering MUST be performed every two years from the date of the previously performed TRA. The TRA MUST be conducted by an Information Security Professional with 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.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS04.04	The vendor MUST have a TRA performed on changes to the EMR Offering under specific conditions and by an independent body.	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 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 The TRA MUST be conducted by an Information Security Professional with one of the following credentials: i. Certified Information Systems Security Professional (CISSP) ii. Certified Information Security Manager (CISM) iii. Certified Information Systems Auditor (CISA) iv. Other credentials may be accepted upon review and consultation with OMD prior to conducting the TRA Note: For TRAs on changes to the EMR Offering, it is not required to be performed by an independent third-party Information Security Professional.	M	P
PS04.05	The vendor MUST submit the TRA report.	The TRA report MUST include all the following information:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		a) Assessor's name b) Assessor's certification type and number c) Identified findings and recommendations d) Scope e) Security controls that were inspected f) Mitigation plan The TRA report MUST be approved by the vendor's Chief Security Officer, or by a representative holding an equivalent role. The vendor MUST provide supporting documentation and substantiation upon request. It is RECOMMENDED that any sensitive or proprietary content, or information that can lead to security risks (e.g., IP address, embedded URLs, etc.) be redacted or omitted.		
PS04.06	The vendor MUST maintain an asset listing for the EMR Offering.	The EMR Vendor MUST ensure that the asset inventory identifies and tracks all components required to deliver and operate the EMR Offering including wherever data traverses. The asset inventory MUST include: a) Asset identifier and description b) Asset owner or responsible party c) Asset classification ratings, including confidentiality, integrity, and availability considerations d) Asset location or hosting environment, where applicable e) Asset valuation to assess the impact in case of damage, compromise, or loss of use Assets recorded in the inventory SHALL be limited to the following categories: i. Information assets (e.g., data repositories and records) ii. Software assets (e.g., applications and system components) iii. Hardware or infrastructure assets (e.g., servers, storage, and network devices) iv. Service assets (e.g., cloud services, hosting services, and integrations supporting the EMR Offering)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS04.07	The vendor MUST maintain a risk listing for the EMR Offering.	The risk listing MUST include identified threats, vulnerabilities, and associated risk ratings. Risk ratings for identified vulnerabilities MUST align with or map to the Common Vulnerability Scoring System (CVSS) v3.1 or higher, as defined by NIST.	M	U
PS04.08	The vendor MUST maintain a security risk mitigation plan.	All identified risks MUST be remediated, mitigated, avoided, transferred, or formally accepted within a defined and prudent timeline based on the severity level. a) Critical and high-severity risks MUST be remediated or mitigated. b) Medium and low-severity risks MUST be documented within the security risk treatment plan, including the planned treatment approach and remediation timeline. c) Any risk that is formally accepted MUST be documented and approved by an authorized security or risk management authority. OMD MAY request the security risk mitigation plan and supporting documentation to verify that identified risks are appropriately documented and addressed.	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 Risks SHOULD be reviewed at least quarterly and risk treatment options updated if required.	M	P

2.5 Security Processes and Controls Audit

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS05.01	The EMR vendor MUST maintain an independent security controls audit or certification demonstrating the effectiveness of security controls supporting the EMR Offering.	One of the following reports or certifications MUST be maintained in current and good standing: a) ISO/IEC 27001 certification, including a Statement of Applicability b) HITRUST R2 certification, including scope and supplementary reports c) SOC 2 Type II audit report Where ISO/IEC 27001 is used: i. ISO/IEC 27001:2022 certification MUST cover the full scope of the EMR Offering and supporting services ii. ISO/IEC 27701 SHOULD be included as an extension, where available, to demonstrate privacy controls for PHI Where SOC 2 Type II is used: I. The audit MUST be performed by an independent AICPA firm II. The audit MUST include the Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy III. The audit MUST cover at least the EMR Offering, infrastructure, and supporting systems	M	N
PS05.02	The security controls audit MUST include all systems, services, and operational processes supporting the EMR Offering.	The audit scope MUST include: a) Scope of vendor services supporting the EMR Offering b) Personnel responsible for operating or supporting the EMR Offering c) Data centres or hosting environments d) Vendor processes, policies, and operational security controls	M	U
PS05.03	The EMR vendor MUST maintain current security audit reports or certifications.	Security certifications or audit reports MUST be maintained according to the following intervals: a) ISO/IEC 27001 certification — every three years b) HITRUST R2 certification — every two years c) SOC 2 Type II audit report — annually Where SOC 2 Type II reports are used to demonstrate compliance with this requirement, the report MUST meet defined assurance expectations.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		The SOC 2 Type II audit MUST: i. Be performed by an independent AICPA firm ii. Include the Trust Services Criteria Covering the EMR Offering, infrastructure, and supporting systems: I. Security II. Availability III. Confidentiality IV. Processing Integrity V. Privacy		
PS05.04	The EMR vendor MUST provide supporting documentation and substantiation of security audit reports or certifications upon request.	The EMR vendor MUST provide documentation demonstrating that the required security audit or certification is current and in good standing. Supporting documentation MUST include: a) A copy of the audit report or certification and the scope of assessment b) The Statement of Applicability, control matrix, or equivalent documentation identifying applicable security controls c) Documentation demonstrating that the EMR Offering and supporting infrastructure are within the scope of the audit or certification d) Evidence of remediation activities or corrective action plans for any identified control deficiencies, where applicable The EMR vendor MUST ensure that documentation provided to OMD is sufficient to verify that the EMR Offering and supporting services are covered by the audit or certification.	M	N
PS05.05	The EMR vendor MUST complete and submit the questionnaire to assess security controls policies and processes.	For criteria not met for any of the questions, the vendor MUST provide the reasoning or details. The EMR vendor MUST re-evaluate and re-submit the questionnaire every two years, from the date of the last submission. The vendor MUST provide supporting documentation and substantiation upon request. Refer to the “Vetting Software Suppliers” section of the provided reference to “Protecting Your Organization from Software Supply Chain Threats” for	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		the list of questions. The questionnaire evaluates the EMR vendor as the “software supplier” and applies to both local and hosted EMR Offerings.		
PS05.06	EMR vendors MUST conduct penetration testing at least annually on their EMR offering.	The EMR Vendor MUST conduct penetration testing to identify, assess, and remediate technical vulnerabilities in EMR solutions prior to deployment and on an ongoing basis for existing deployments. EMR vendors MUST perform penetration testing on EMR solutions to identify, assess, and remediate technical vulnerabilities in their systems prior to deployment and on an ongoing basis for existing deployments. a) Pre-deployment: In an environment simulating a typical clinic LAN setup, before handover to the client (for new implementations). b) Ongoing: At least annually and after any major system change for already deployed solutions. c) Assess the application for vulnerabilities exploitable from within the LAN, including but not limited to: a. Authentication and authorization weaknesses b. Injection flaws (SQL injection, command injection) c. Insecure default configurations d. Weak or unsupported encryption for data at rest and in transit d) Testing must be completed in accordance with one of the following accepted methodologies: a. Open Web Applications Security Project (OWASP) b. Penetration Testing Execution Standards (PTES) c. NIST SP 800-115 d. Open Source Testing Methodology Manual (OSSTMM) e) Penetration testing MUST be conducted by an independent third-party Information Security Professional whose credentials can be verified. Testing scope SHOULD consider deployment model differences: i. For Local EMR Offerings: testing SHOULD focus on the application layer. ii. For Hosted EMR Offerings: testing SHOULD include the application layer and, where applicable, the network layer.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
PS05.07	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
PS05.08	The EMR 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 current and good standing. a) Certified Ethical Hacker (CEH) b) Offensive Security Certified Professional (OSCP) c) GIAC Penetration Tester (GPEN) Other credentials may be accepted upon review and consultation with OMD prior to conducting testing. The Information Security Professional conducting penetration testing MUST be from an external organization specializing in information security reviews, and whose credentials can be verified.	M	N
PS05.09	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	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		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 TRA checklist, MUST be approved by the vendor's Chief Security Officer, or equivalent role. Refer to the penetration testing checklist included in this specification for guidance on information to include in the penetration testing report. Any sensitive or proprietary content or information that can lead to asset identification, or security risks (e.g., IP address, embedded URLs, etc.) SHOULD be redacted (i.e., concealed, omitted or deleted).		
PS05.10	The vendor MUST document a security risk treatment plan for all vulnerabilities identified.	Vulnerability severity ratings MUST align with or map to the CVSS v3.1 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

2.6 Vulnerability Scans

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. The EMR Vendor MUST ensure that vulnerability assessments are performed in accordance with the following requirements: a) Scope of the scans performed, including systems, services, and infrastructure supporting the EMR Offering b) Identified vulnerabilities, including severity classification c) Date of the scans performed or the frequency of scheduled scan d) Remediation plan for identified vulnerabilities e) Evidence of remediation actions taken, where applicable	M	N
PS06.02	The vendor MUST submit a report of the vulnerability and configuration scans performed to OMD.	The report MUST identify all of the following information: a) Scope of the scans performed, including the systems and services assessed b) Identified vulnerabilities, including severity classification c) Date of the scans performed or the frequency of scheduled scans d) Remediation plan, including evidence of remediation actions taken The report MUST be provided to OMD every two years. OMD MAY request an ad-hoc report at any time. Sensitive technical information (e.g., specific vulnerability details, IP addresses, or system identifiers) SHOULD NOT be included in the submitted report.	M	N
PS06.03	The vendor MUST document a security risk mitigation plan for all vulnerabilities identified by a vulnerability assessment, to be provided upon request.	Vulnerability severity ratings MUST align with or map to the Common Vulnerability Scoring System (CVSS) v3.1 or higher, as defined by NIST. Refer to the "Vulnerability Metrics".	M	U

		Known or identified vulnerabilities MUST be remediated or mitigated within a defined and prudent timeline based on severity level. The security risk mitigation plan MUST document: a) Vulnerabilities identified through malware detection, scanning controls and regular security assessments b) The associated severity classification c) The proposed remediation or mitigation strategy d) The planned remediation timeline OMD maintains the discretion to review the security risk mitigation plan and supporting documentation to ensure that identified vulnerabilities are appropriately addressed.		
--	--	---	--	--

3. APPENDICES

3.1 Appendix A: Glossary

TERM	DEFINITION
All persons	The vendor, including its staff, agents, suppliers and electronic service providers. Clinic employees, staff, technical staff or agents that provide services to the clinic.
Authentication Assurance Level (AAL)	A classification defined in NIST SP 800-63 describing the strength of authentication mechanisms (e.g., AAL2, AAL3).
Attribute-Based Access Control (ABAC)	An access control model where access decisions are based on attributes such as user, device, or context.
Agent	A person or organization authorized to perform services or activities on behalf of the EMR Vendor or a Health Information Custodian (HIC).
American Institute of Certified Public Accounts (AICPA)	The governing body that established the Trust Services Criteria and the auditing standards used to evaluate controls related to SOC 2 Type 2.
Application Programming Interface (API)	A set of rules and interfaces that allow systems to communicate and exchange data.

TERM	DEFINITION
Asset	Any data, system, application, service, or infrastructure component required to deliver or support the EMR Offering.
Asset Inventory	A maintained listing of all assets required to deliver and operate the EMR Offering.
Audit Trail	A chronological record of system activities enabling reconstruction of events.
Electronic Medical Record (EMR)	A digital system used to create, store, manage, and access patient medical records.
EMR Offering	The EMR solution, including application software, components, and interfaces used to deliver EMR functionality.
EMR Vendor	The organization responsible for developing, operating, maintaining, or supporting the EMR Offering.
Electronic Service Provider	The organization that provides electronic services supporting the storage, processing, transmission, or management of information for the EMR Offering.
Multi-Factor Authentication (MFA)	An authentication method requiring two or more distinct factors to verify identity.
Personal Health Information (PHI)	Identifying information about an individual's health or health care, as defined under applicable privacy legislation (e.g., PHIPA).
Personal Health Information Protection Act (PHIPA)	Ontario legislation governing the collection, use, and disclosure of personal health information.
Privacy Impact Assessment (PIA)	A formal assessment evaluating how personal information is collected, used, disclosed, and protected.
Privileged ID	A user account with elevated permissions beyond standard users.
Program Office	The group of Agents and Electronic Service Providers that support the EMR Offering, including operations, privacy, security, and program administration activities.
Role-Based Access Control (RBAC)	An access control model where permissions are assigned to roles rather than individual users.
Service ID	A non-interactive account used by applications or services to perform automated processes.
User ID (managed by vendor)	Credentials within the EMR Offering that are managed by the vendor.

TERM	DEFINITION
Non-Interactive	Access does not require a user interface to login.

3.2 Appendix B: Minimum Password Requirements

The following is a list of minimum password requirements for IDs associated with the Program Office connected to the hosted EMR Offering.

For the purposes of this appendix, the Program Office refers to the group of Agents and Electronic Service Providers who support the EMR Offering, including activities related to operations, privacy, security, and program administration.

	Personal IDs & Privileged IDs	Service IDs
Length	Be at least 8 characters when used with multi-factor authentication (MFA). Where passwords are used as the sole authentication factor, passwords MUST be at least 15 characters.	Be at least 15 characters and randomly generated where possible.
Complexity	Passwords SHOULD support the use of printable ASCII characters, including spaces. Mandatory composition rules requiring uppercase, lowercase, numeric, or special characters SHOULD NOT be enforced.	Passwords SHOULD be randomly generated and stored securely (e.g., credential vault or secrets manager).

	Personal IDs & Privileged IDs	Service IDs
Additional Password Attributes	- Where available, software that prevents the use of commonly used, weak, or compromised passwords MUST be used. - Passwords MUST NOT contain easily guessed information such as names, usernames, or publicly known personal information. - Initial or temporary passwords MUST be unique, not guessable, follow the password requirements, and be communicated securely. - Passwords MUST NOT be blank and null passwords MUST NOT be used. Guest passwords MUST be disabled.	Service credentials MUST be protected using secure credential storage mechanisms. Hard-coded credentials MUST NOT be stored in applications, scripts, or configuration files
Expiration	Passwords SHOULD NOT expire on a fixed schedule. Password changes MUST occur if compromise is suspected or detected.	Service IDs are not required to be changed on a scheduled basis; however credentials SHOULD be rotated when systems or technologies change or when compromise is suspected.
Account Lockout	Authentication systems MUST implement protections against repeated failed login attempts (e.g., lockout thresholds or rate limiting).	
Lockout duration	Until manually unlocked by: - An administrator, or - A self-service password reset facility. – OR – Unlocked after a minimum of 30 minutes	
History	Prevent reuse of at least the previous 10 passwords.	
Minimum Age	Not required. Users MUST be able to change passwords immediately if compromise is suspected.	

Note: While these requirements represent OMD's preferred standards, EMR vendors SHOULD align with current industry security guidance where applicable.

3.3 Appendix C: Approved Cryptographic Algorithms

Algorithm	Minimum Key Length	Appropriate Usage	
Symmetric Key Algorithms			
AES	128-bit minimum (256-bit recommended)	Data encryption: • Session • Storage ○ Backup ○ Archival	Key encryption: • Session • Storage ○ Backup ○ Archival
AES-GCM	128-bit minimum	Authenticated encryption for data in transit and storage.	
Asymmetric Key Algorithms			
Elliptic Curve Cryptography (ECC)	224-bit minimum (e.g., P-256 recommended)	Data encryption: • Session • Storage ○ Backup ○ Archival • Digital Signature	Key encryption: • Session • Storage ○ Backup ○ Archival • Session key establishment
RSA	2048-bits	Data encryption: • Session • Storage ○ Backup ○ Archival • Digital Signature	Key encryption: • Session • Storage ○ Backup ○ Archival • Session key establishment

Algorithm	Minimum Key Length	Appropriate Usage
MACs and Hashes		
AES CMAC	128-bits	Message authentication
HMAC-SHA-256 or stronger	N/A	Message authentication
SHA-256 / SHA-384 / SHA-512	N/A	Message digest and integrity validation
Digital Signatures		
Elliptic Curve DSA	224-bits minimum (P-256 recommended)	Digital Signature
RSA PSS	2048-bits	Digital Signature
Digital Certificates		
X.509 v3 compliant	N/A	Binds a public key with a specific identity
Key Transport/Agreement Algorithms		
Diffie-Hellman	2048-bits minimum	Digital Session key establishment
Elliptic Curve Diffie-Hellman	P-256 minimum	Digital Session key establishment
Cryptographic Protocols		
TLS 1.2 and higher	N/A	Protocol to authenticate and encrypt communication between authenticated parties

Note: While these requirements represent OMD's preferred standards, EMR vendors SHOULD align with current industry security guidance where applicable.