

EMR Hosting

Requirements

September 11, 2026

Document Version & Status: 1.5 – DFC



1. Table of Contents

1. TABLE OF CONTENTS	2
1. INTRODUCTION.....	3
1.1 PURPOSE	3
1.2 APPLICABILITY.....	3
1.3 VERSION HISTORY	4
2. EMR SPECIFICATION SCOPE	13
2.1 RELATED DOCUMENTS, REFERENCES AND SOURCES.....	14
3. EMR REQUIREMENTS	16
4. HOSTING MODEL AND ACCOUNTABILITY	17
5. SECURITY CONTROLS.....	23
5.1 NETWORK AND INFRASTRUCTURE SAFEGUARDS.....	23
5.2 IDENTITY AND ACCESS CONTROLS	28
5.3 CRYPTOGRAPHY	39
5.4 VULNERABILITY AND REMEDIATION MANAGEMENT.....	57
5.5 ENDPOINT AND PERIMETER PROTECTION	63
6. LOGGING, MONITORING AND INCIDENT MANAGEMENT	67
7. BUSINESS CONTINUITY AND DISASTER RECOVERY.....	76
8. ACCEPTABLE USE OF INFORMATION AND INFORMATION TECHNOLOGY	85
9. INFORMATION AND ASSET MANAGEMENT	93
10. PHYSICAL SECURITY.....	94
11. SUPPLIER AND THIRD-PARTY MANAGEMENT	101
12. COMPLIANCE AND ASSURANCE	105
13. APPENDICES.....	107
13.1 APPENDIX A: GLOSSARY	107
13.2 APPENDIX B: MINIMUM PASSWORD REQUIREMENTS.....	108
13.3 APPENDIX C: INFORMATION SECURITY INCIDENT MANAGEMENT	110

13.4	APPENDIX D: APPROVED CRYPTOGRAPHIC ALGORITHMS	114
13.5	APPENDIX E: SECURITY LOGGING AND MONITORING	116
13.6	APPENDIX F: INFORMATION ASSET MANAGEMENT	118
13.7	APPENDIX G: PHYSICAL SECURITY ZONES	123

1. INTRODUCTION

1.1 Purpose

The purpose of this document is to define the hosting requirements applicable to an EMR Vendor that delivers a hosted EMR Offering.

Hosting, for the purposes of this specification, refers to the business and technical services provided by the EMR Vendor to make the EMR Vendor available to subscribers through a networked environment, including vendor-managed and cloud-based infrastructure models.

This specification defines the requirements and expectations for hosting an OntarioMD certified EMR Vendor and establishes the safeguards and operational controls necessary to support the protection, availability, and reliability of the hosted EMR environment.

The target audience for this document is vendors that want to have their hosted EMR Offering certified by OMD. It is assumed that readers of this document have a background in cloud technology and information security.

1.2 Applicability

These hosting requirements apply to all environments used to host, process, store, transmit, or support data associated with the EMR Vendor, including:

- Production environments
- Backup environments
- Disaster recovery environments
- Supporting infrastructure and management components

The requirements apply regardless of whether the hosting infrastructure is:

- On-premise environments (e.g., installations within a healthcare organization's facilities)
- Vendor-managed private data centres

- Managed Service Provider (MSP) environments
- Public or private cloud environments

The requirements apply regardless of whether the hosting infrastructure is:

- Operated directly by the EMR Vendor; or
- Provided by third-party service providers (e.g., cloud providers, MSPs) under the accountability of the EMR Vendor

Where possible, requirements are defined to apply consistently across all deployment models. Where a requirement is specific to a particular deployment model, its applicability is explicitly identified within the relevant section.

The EMR Vendor remains fully accountable for ensuring that all hosting environments supporting the EMR Offering comply with the requirements defined in this document, including environments operated by third parties.

1.3 Version History

VERSION	REVISION DATE	REVISION NOTES
1.5	2026-09-11	The Hosting Specification has been restructured with a new table of contents. Requirements have been updated, consolidated, moved, or retired. Guidelines have been introduced across all requirements to improve clarity, consistency, and alignment with industry standards. a) Updated HST01.01: Requirement refined to strengthen centralized monitoring across infrastructure, platform, and application layers. Requirement moved to Logging, Monitoring and Incident Management. b) Updated HST01.02: Requirement revised and guidelines updated to clarify that notification services are intended to support service continuity and operational awareness. Requirement moved to Business Continuity and Disaster Recovery. c) Updated HST01.07: Requirement incorporated into HST08.04 with HST08.08 to consolidate business continuity planning requirements and has been moved to the Business Continuity Section. d) Updated HST01.08: Requirement and guidelines revised to clarify Point-in-Time Recovery expectations and alignment with recovery objectives. Renumbered as HST08.10 and moved to Business Continuity and Disaster Recovery. e) Updated HST02.01, HST02.02: Added guidelines for clarity. Requirements moved to Hosting Model and Accountability. f) Updated HST02.03: Requirement moved to Logging, Monitoring and Incident Management to align with operational procedures for monitoring, alerting, and escalation. g) Updated HST02.04: Requirement moved to Identity and Access Management. Guidelines updated to align with access control and least privilege principles.

VERSION	REVISION DATE	REVISION NOTES
		h) Updated HST02.05, HST02.06: Requirements merged to remove duplication and streamline network control expectations. Requirement moved to Network and Infrastructure Safeguards. i) Updated HST02.07–HST02.23: Guidelines updated to align with industry-standard controls for network protection, segmentation, and secure communications. Requirements reorganized across Network and Infrastructure Safeguards, Endpoint and Perimeter Controls, and Cryptography to improve logical grouping. j) Updated HST02.24–HST02.47: Guidelines updated to align with vulnerability management, flaw remediation, and configuration management practices. Requirements consolidated where duplication existed and moved to Vulnerability and Patch Management. k) Updated HST02.25, HST02.26, HST02.29, HST02.30, HST02.41, HST02.45: Requirements merged to eliminate overlapping controls and improve clarity. a. Updated HST02.25 and HST02.26: Requirements merged and renumbered as HST06.09 to consolidate IDS/IPS alert generation, alert threshold configuration, and security monitoring expectations. b. Updated HST02.29 and HST02.30: Requirements merged and renumbered as HST06.10 to consolidate malware definition and detection-software update requirements. c. Updated HST02.41 and HST02.45: Requirements merged and renumbered as HST05.11 to consolidate security patch management and compensating-control requirements. l) Updated HST02.27: Requirement refined to strengthen incident handling expectations for IDS and IPS events. Requirement moved to Logging, Monitoring and Incident Management to align with incident response processes. m) Updated HST02.28: Added malware guidance and removed alternative solutions like thin clients. n) Updated HST02.31: Requirement refined to clarify malware scanning, real-time protection, and isolation and remediation expectations for systems not protected by real-time controls. o) Updated HST02.35, HST02.36: Requirements moved to Privacy and Security Requirements as they relate to enterprise-level privacy and governance controls. p) Updated HST02.37: Requirement retired due to overlap with existing vulnerability and risk management controls. q) Updated HST02.48–HST02.54: Requirements moved to Business Continuity and Disaster Recovery. Guidelines updated to clarify backup, recovery, and contingency planning expectations. r) Updated former HST03.03 and HST03.09: Requirements renumbered as HST11.03 and HST11.12, respectively, and retained with a status of “Retired” to preserve historical traceability. The requirements were retired due to redundancy and overlap with broader physical security controls. s) Updated HST03.05–HST03.18: Guidelines added or refined to improve clarity and ensure applicability to third-party hosting providers. t) Updated HST03.17: Requirement enhanced to ensure that exceptions to layered security controls are supported by a formal threat and risk assessment and appropriate compensating controls. u) Updated HST05.04–HST05.42: Guidelines added and updated to align with identity, authentication, and access control best practices. Requirements consolidated and repositioned under Identity and Access Management to improve logical grouping.

VERSION	REVISION DATE	REVISION NOTES
		v) Updated HST05.21, HST05.27, HST05.39: Requirements retired due to overlap with existing identity and access management controls. w) Updated HST05.24–HST05.34: Requirements moved to Privacy and Security Requirements under Data and System Access Management to align with enterprise-level access governance. x) Updated HST06.06: Requirement moved to Cryptography. Guidelines updated to align with protection of sensitive data and communications. y) Updated HST08.03, HST08.05: Requirements merged to consolidate high availability, failover, and transaction recovery expectations. Requirement moved to Business Continuity and Disaster Recovery. z) Updated HST08.04: Requirement refined to clarify risk reduction expectations related to system reliability, compatibility, and capacity planning. Requirement moved to Business Continuity and Disaster Recovery. - aa) Updated HST08.06: Requirement moved to Business Continuity and Disaster Recovery. Guidelines updated to clarify network resilience and redundancy expectations. - bb) Updated HST08.07: Requirement retired due to overlap with logging, monitoring, and incident management controls, specifically fault detection and response. - cc) Updated HST09.01–HST09.53: Guidelines added or refined to align with cryptographic best practices, including key management, lifecycle controls, protection mechanisms, and governance expectations. - dd) Updated HST09.22, HST09.23, HST09.24, HST09.32: Requirements retired due to redundancy or consolidation into broader cryptographic controls. - ee) Updated HST09.50: Guidelines updated to modernize cryptographic key handling terminology and remove dependency on retired information asset classification references. - ff) Updated HST10.01–HST10.30: Requirements reviewed and refined to improve clarity, consistency, and completeness of logging, monitoring, and incident management controls. Selective consolidation was applied where duplication existed, particularly in log protection, monitoring, and lifecycle management. - gg) Updated HST11.01–HST11.03: Requirements refined to clarify supplier classification, documentation, and risk assessment practices. Requirements moved to Supplier and Third-Party Management to support a structured vendor lifecycle approach. - hh) Updated HST11.04: Requirement retired due to overlap with HST11.02. Contractual, documentation, and service definition controls were consolidated. ii) Updated HST11.05: Requirement refined to clarify third-party onboarding and pre-access control expectations, including validation of security and privacy controls prior to granting access. - jj) Updated HST11.06: Requirement retired due to overlap with HST11.03. Threat and risk assessment controls were consolidated. - kk) Updated HST11.07: Guidelines updated to clarify data ownership and disposition requirements during third-party termination. Data ownership expectations have been integrated into data transfer and disposal controls to ensure alignment with contractual, retention, and privacy obligations. - ll) Updated HST11.08: Requirement refined to clarify third-party contingency arrangements and ensure alignment with business continuity and disaster recovery programs. - mm) New Requirement HST01.09: Introduced to define requirements for documenting geographic data residency and processing locations for the EMR Offering, including primary, secondary, and third-party hosting regions.

VERSION	REVISION DATE	REVISION NOTES
		nn) New Requirement HST01.10: Introduced to establish that the EMR vendor retains full accountability for the confidentiality, integrity, and availability of the EMR Offering, including when third-party providers are used. oo) New Requirement HST01.11: Introduced to define requirements for documenting the shared responsibility model, including the division of security and operational responsibilities between the EMR vendor and subscribers. pp) New Requirement HST01.12: Introduced to require identification of third-party infrastructure and cloud service providers supporting the EMR Offering, including service type and hosting regions. qq) New Requirement HST01.13: Introduced to require maintenance of current assurance evidence for third-party infrastructure and cloud service providers supporting the EMR Offering. rr) New Requirement HST06.08: Introduced to define network segmentation requirements for unmanaged, insecure, or non-trusted devices, including IoT, to prevent unauthorized access to systems supporting the hosted EMR environment. ss) New Requirement HST13.01: Introduced to define evidence requirements for alignment with recognized security and cloud frameworks. tt) New Requirement HST13.02: Introduced to define independent third-party assurance requirements, including SOC 2 Type II reporting. Updated Appendices: uu) Appendix labelling updated for consistency: i. Appendix C: Minimum Password Requirements relabelled as Appendix B. ii. Appendix E: Information Security Incident Management relabelled as Appendix C. iii. Appendix F: Approved Cryptographic Algorithms relabelled as Appendix D. iv. Appendix G: Security Logging and Monitoring relabelled as Appendix E. v. Appendix B: Physical Security relabelled as Appendix G. vi. Appendix D: Information Asset Management relabelled as Appendix F. ggg) Updated Requirement IDs: • HST01.02 from HST01.04 • HST01.03 from HST01.05 • HST01.04 from HST01.06 • HST01.05 from HST01.09 • HST01.06 from HST01.11 • HST01.07 from HST02.01 • HST01.08 from HST02.02 • HST02.02 from HST02.07 • HST02.03 from HST02.08 • HST02.05 from HST02.10 • HST02.06 from HST02.13 • HST02.07 from HST02.17 • HST02.08 from HST02.18 • HST02.09 from HST02.19

VERSION	REVISION DATE	REVISION NOTES
		• HST02.10 from HST02.23 • HST02.11 from HST02.32 • HST03.01 from HST05.05 • HST03.02 from HST05.07 • HST03.03 from HST05.09 • HST03.04 from HST05.11 • HST03.05 from HST05.15 • HST03.06 from HST05.16 • HST03.07 from HST05.17 • HST03.08 from HST05.18 • HST03.09 from HST05.19 • HST03.10 from HST05.20 • HST03.11 from HST05.22 • HST03.12 from HST05.23 • HST03.13 from HST05.35 • HST03.14 from HST05.36 • HST03.15 from HST05.37 • HST03.16 from HST05.38 • HST03.17 from HST05.40 • HST03.18 from HST05.41 • HST03.19 from HST05.42 • HST03.20 from HST02.04 • HST03.21 from HST05.06 • HST03.22 from HST05.10 • HST03.23 from HST05.12 • HST03.24 from HST05.13 • HST03.25 from HST05.24 • HST03.26 from HST05.25 • HST03.27 from HST05.26 • HST03.28 from HST05.28 • HST03.29 from HST05.29 • HST03.30 from HST05.30 • HST03.31 from HST05.31 • HST03.32 from HST05.32 • HST03.33 from HST05.33 • HST03.34 from HST05.34 • HST03.35 from HST05.14 • HST04.01 from HST02.11 • HST04.02 from HST02.21 • HST04.03 from HST06.06 • HST04.04 from HST09.01

VERSION	REVISION DATE	REVISION NOTES
		• HST04.05 from HST09.02 • HST04.06 from HST09.03 • HST04.07 from HST09.04 • HST04.08 from HST09.05 • HST04.09 from HST09.06 • HST04.10 from HST09.07 • HST04.11 from HST09.08 • HST04.12 from HST09.09 • HST04.13 from HST09.10 • HST04.14 from HST09.11 • HST04.15 from HST09.12 • HST04.16 from HST09.13 • HST04.17 from HST09.14 • HST04.18 from HST09.15 • HST04.19 from HST09.16 • HST04.20 from HST09.17 • HST04.21 from HST09.18 • HST04.22 from HST09.19 • HST04.23 from HST09.20 and HST09.22 • HST04.24 from HST09.21 • HST04.25 from HST09.25 • HST04.26 from HST09.26 • HST04.27 from HST09.27 • HST04.28 from HST09.28 • HST04.29 from HST09.29 • HST04.30 from HST09.30 • HST04.31 from HST09.31 • HST04.32 from HST09.33 • HST04.33 from HST09.34 • HST04.34 from HST09.35 • HST04.35 from HST09.36 • HST04.36 from HST09.37 • HST04.37 from HST09.38 • HST04.38 from HST09.39 • HST04.39 from HST09.40 • HST04.40 from HST09.41 • HST04.41 from HST09.42 • HST04.42 from HST09.43 • HST04.43 from HST09.44 • HST04.44 from HST09.45 • HST04.45 from HST09.46

VERSION	REVISION DATE	REVISION NOTES
		• HST04.46 from HST09.47 • HST04.47 from HST09.48 • HST04.48 from HST09.49 • HST04.49 from HST09.50 • HST04.50 from HST09.51 • HST04.51 from HST09.52 • HST04.52 from HST09.53 • HST05.01 from HST02.24 • HST05.02 from HST02.28 • HST05.03 from HST02.29 • HST05.04 from HST02.31 • HST05.05 from HST02.32 • HST05.06 from HST02.33 • HST05.07 from HST02.34 • HST05.08 from HST02.38 • HST05.09 from HST02.39 • HST05.10 from HST02.40 • HST05.11 from HST02.41 • HST05.12 from HST02.42 • HST05.13 from HST02.43 • HST05.14 from HST02.44 • HST05.15 from HST02.46 • HST05.16 from HST02.47 • HST06.01 from HST02.16 • HST06.02 from HST02.12 • HST06.03 from HST02.10 • HST06.04 from HST02.14 • HST06.05 from HST02.15 • HST06.06 from HST02.20 • HST07.01 from HST01.01 • HST07.02 from HST02.03 • HST07.03 from HST10.01 • HST07.04 from HST10.03 • HST07.05 from HST10.04 • HST07.06 from HST10.06 • HST07.07 from HST10.07 • HST07.08 from HST10.08 • HST07.09 from HST10.09 • HST07.10 from HST10.10 • HST07.11 from HST10.11 and HST10.12 • HST07.12 from HST10.14

VERSION	REVISION DATE	REVISION NOTES
		• HST07.13 from HST10.15 • HST07.14 from HST10.18 • HST07.15 from HST10.21 • HST07.16 from HST10.22 • HST07.17 from HST10.23 • HST07.18 from HST10.24 • HST07.19 from HST10.27 • HST07.20 from HST10.25 and HST10.26 • HST07.21 from HST10.28 • HST07.22 from HST02.27 • HST08.01 from HST01.07 • HST08.02 from HST08.02 • HST08.03 from HST01.02 • HST08.04 from HST01.07 and HST08.08 • HST08.05 from HST08.09 • HST08.06 from HST08.10 • HST08.07 from HST08.11 • HST08.08 from HST08.12 • HST08.09 from HST08.13 • HST08.10 from HST01.08 • HST08.11 from HST02.48 • HST08.12 from HST02.49 • HST08.13 from HST02.50 • HST08.14 from HST02.51 • HST08.16 from HST02.53 • HST08.17 from HST02.54 • HST08.18 from HST08.03 • HST08.19 from HST08.04 • HST08.20 from HST08.06 • HST08.22 from HST02.55 • HST09.01 from HST04.01 • HST09.02 from HST04.02 • HST09.03 from HST04.03 • HST09.04 from HST04.04 • HST09.05 from HST04.05 • HST09.06 from HST04.06 • HST09.07 from HST04.07 • HST09.08 from HST04.08 • HST09.09 from HST04.09 • HST09.10 from HST04.10 • HST09.11 from HST04.11

VERSION	REVISION DATE	REVISION NOTES
		• HST09.12 from HST04.12 • HST09.13 from HST04.13 • HST09.14 from HST04.14 • HST09.15 from HST04.15 • HST09.16 from HST04.16 • HST09.17 from HST04.17 • HST09.18 from HST04.18 • HST09.19 from HST04.19 • HST09.20 from HST04.20 • HST09.21 from HST04.21 • HST09.22 from HST04.22 • HST09.23 from HST04.23 • HST09.24 from HST04.24 • HST09.25 from HST04.25 • HST09.26 from HST04.26 • HST09.27 from HST04.27 • HST09.28 from HST04.28 • HST09.29 from HST04.29 • HST09.30 from HST04.30 • HST09.31 from HST04.31 • HST09.32 from HST04.32 • HST09.33 from HST04.33 • HST10.01 from HST06.01 • HST10.02 from HST06.02 • HST10.03 from HST06.03 • HST10.04 from HST06.04 • HST10.05 from HST06.05 • HST10.06 from HST06.07 • HST11.01 from HST03.01 • HST11.02 from HST03.02 • HST11.04 from HST03.04 • HST11.05 from HST05.01 • HST11.08 from HST03.05 • HST11.09 from HST03.06 • HST11.10 from HST03.07 • HST11.11 from HST03.08 • HST11.13 from HST03.10 • HST11.14 from HST03.11 • HST11.15 from HST03.12 • HST11.16 from HST03.13 • HST11.17 from HST03.14

VERSION	REVISION DATE	REVISION NOTES
		• HST11.18 from HST03.15 • HST11.19 from HST03.16 • HST11.20 from HST03.17 • HST11.21 from HST03.18 • HST11.22 from HST03.19 • HST12.01 from HST11.01 • HST12.02 from HST11.02 and HST11.04 • HST12.03 from HST11.03 and HST11.06 • HST12.04 from HST11.07 • HST13.03 from HST11.05 • HST13.04 from HST11.08

2. EMR SPECIFICATION SCOPE

The EMR hosting requirements expressed within this document are applicable to the following services provided by the vendor:

- Central Monitoring
- Client Notification Service
- Help Desk Services
- Release Notifications
- Implementation Plan
- Training Services
- Business Continuity and Data Recovery
- Accessibility Support
- Provincial EHR Solutions and Services Interoperability
- Service Level Management

The EMR information security requirements expressed within this document are aligned with information security policies, based on ISO 27002 control objectives, and cover the following topics:

- Hosting Model and Accountability
- Security Controls
 - Network and Infrastructure Safeguards
 - Identity and Access Controls
 - Cryptography

- Vulnerability and Remediation Management
- Endpoint and Perimeter Controls
- Logging, Monitoring and Incident Management
- Business Continuity and Disaster Recovery
- Suppliers and Third-Party Management
- Compliance and Assurance

2.1 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
Regulatory / Health	Ontario Health, Electronic Health Record Retention Policy Electronic Health Record Retention Policy and Procedure Ontario Health	N/A	Current
Government Policy	Treasury Board Policy on Service and Digital (Treasury Board of Canada Secretariat) Treasury Board Policy on Service and Digital	Current	2020
Security Framework	NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	Rev. 5	2020
Security Guidance	NIST SP 800-92 – Guide to Computer Security Log Management https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf	N/A	2006
Security Guidance	Government of Canada Event Logging Guidance Government of Canada Event Logging Guidance	Current	2024

CATEGORY	NAME	VERSION	DATE
Security Framework	ISO/IEC 27001 – Information Security Management Systems https://www.iso.org/standard/27001	2022	2022
Security Framework	ISO/IEC 27002 – Information Security Controls https://www.iso.org/standard/27002	2022	2022
Security Framework	ISO/IEC 27017 – Code of Practice for Information Security Controls for Cloud Services https://www.iso.org/standard/27017	2015	2015
Cloud Security Framework	CSA Cloud Controls Matrix (CCM) https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4	v4	Current
Cloud Security Framework	CSA Consensus Assessments Initiative Questionnaire (CAIQ) https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v4	v4	Current
Assurance / Audit	SOC 2 Type II (AICPA Trust Services Criteria – Security, Availability, Confidentiality) https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2	N/A	Current

3. EMR REQUIREMENTS

This section consists of the EMR requirements for EMR Hosting Services.

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

P = Previous requirement

U = Updated requirement

R = Retired requirement

OMD #:

A unique identifier that identifies each requirement within OMD's EMR Requirements 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 contain additional instructions or detail about the high-level requirement. The text in both columns are considered requirement statements.

4. Hosting Model and Accountability

To establish a transparent operational baseline, this section outlines the logical hosting architecture and the Shared Responsibility Model, clarifying the distinct security obligations held by the EMR vendor versus those inherited from the underlying Cloud Service Provider (CSP) and/or Managed Service Provider (MSP).

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST01.01	Help Desk The EMR vendor MUST have a centralized, province-wide Help Desk so that their subscribers and EMR users can create and track incidents and service requests. The EMR Vendor MUST provide a centralized Help Desk that enables all subscribers and EMR users to create, submit, and track incidents and service requests. The Help Desk MUST serve as a single point of contact for support across the entire province.	The incident management system MUST include at a minimum: a) Call logging b) Ticketing, and reporting by service categories (e.g., server, network, applications, privacy, security, performance, availability of interfaces to Provincial EHR Solutions and Services and other interfaces, local IT support) c) Systematic tracking and prioritizing calls using severity levels Subscribers and EMR users MUST have the ability to create service requests via telephone, voicemail and email. Subscribers and EMR users MUST have self-management options to perform common service requests such as: a) Open, view and track service request tickets online b) User password reset	M	U
HST01.02	Release Notes A description of all new and updated functionality and fixes for an EMR Offering release MUST be documented by the vendor and published to subscribers and EMR users of that EMR Offering prior to all implementations or upgrades. The EMR Vendor MUST document all new and updated functionality, enhancements, and fixes included in each EMR Offering release. This documentation MUST be	Release Notes MUST at a minimum, contain the following information for the EMR Offering being implemented or upgraded: a) Features and changes (new features, defects corrected, caveats, etc.) b) Outstanding issues (unresolved defects, if any, workarounds, installation issues, etc.) c) System requirements (hardware, resources, software, third-party platforms or modules, fax servers, scanners, printers, with vendor's version numbers and dates)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	published and made available to all subscribers and EMR users prior to any implementation or upgrade of the EMR Offering.	d) Installation instructions, notes, guide (how to install, how to obtain the guide, etc.) e) Upgrade instructions/notes/guide (how to upgrade, how to obtain the guide, etc.) f) Known issues or limitations of the upgrade, (e.g., a known bug, etc.) g) Contact information for support h) Release version and date of availability i) Other resources and links The following information is also helpful to include: a) Troubleshooting b) Frequently Asked Questions (FAQs)		
HST01.03	Implementation Plan The EMR Vendor MUST publish implementation and upgrade plans to all affected subscribers and EMR users prior to: a) The initial implementation of the EMR Offering; and b) Any subsequent update or upgrade of the EMR Offering. These plans MUST be communicated in advance to ensure subscribers and EMR users are informed of timelines, impacts, and required actions.	An implementation or upgrade plan MUST include at a minimum: a) The purpose of the implementation or upgrade b) When the implementation or upgrade will be performed and its planned duration c) Any potential impacts to EMR users' medical practices during the implementation or upgrade d) Any preparation required in advance of the implementation or upgrade e) Who and how to contact support during and after the implementation or upgrade f) How to receive training (if applicable and provided) If the implementation plan involves the migration of data from another EMR Offering, the plan MUST also provide a detailed plan on how data will be extracted and securely transferred to the subscriber, subscriber's agent or new vendor. The plan MUST include: a) roles and responsibilities of all parties b) a schedule c) vendor's approach to the migration of data d) vendor services related to data preparation, data migration and subsequent subscriber acceptance	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST01.04	Training for Enhanced Use EMR Vendor's training services made available to its subscribers and EMR users MUST include: a) Training on the standard features and functionality for an EMR Offering; and b) Customized or advanced training options on the operation of vendor's EMR Offerings.	In addition to training on the standard features and functionality for an EMR Offering, the EMR vendor MUST also provide EMR user training on advanced techniques used to leverage one or more specific features of an EMR Offering in a medical practice (e.g., performing analytics and reporting, customizing practice workflows, optimizing the use of clinical forms). This enhanced training MAY be provided through pre-established training content or be customizable as agreed to by the vendor and the subscriber and delivered through one or more formats (e.g., online training, online training video, computer-based training, in-person training). Subscribers and users have at their option, the ability to test features or functionality of an EMR Offering using simulated medical practice and/or simulated patient data.	M	U
HST01.05	Accessibility The EMR Offering MUST be accessible to authorized users from multiple physical locations using one or more supported client access methods, in accordance with defined security and access control requirements.	EMR users may require access to the EMR Offering from multiple physical locations, including but not limited to: a) Primary medical practice location b) Satellite offices c) Hospitals d) Other authorized remote locations Client platform technologies MAY include: a) Microsoft Windows b) macOS c) Mobile platforms (e.g., iOS, Android) d) Other vendor-supported operating systems The EMR Offering MUST be accessible using at least one of the following access methods: a) Modern web browsers (e.g., Chromium-based browsers, Firefox, Safari) b) Remote desktop or virtual workspace solutions (e.g., RDS, Citrix, or equivalent)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) Native client applications connecting to a hosted or remote environment		
HST01.06	Service Levels The hosted EMR Offering MUST be highly available, and meet requirements for system performance-	The EMR Offering MUST provide $\geq 99.9\%$ availability to subscribers per calendar month (excluding scheduled downtime). The time to complete the following MUST be ≤ 3 seconds for 90% of occurrences, per calendar month: a) Time from the EMR login screen to the main page b) Time to open appointments c) Time to display Cumulative Patient Profile (CPP) d) Time to display a table of lab results Time is measured from when the user initiates the related request, to when the expected page completes loading. It is not acceptable to provide server-side response times. The Service Level Agreement for the EMR Offering MUST include Help Desk service levels (e.g., call answer time, time to resolution, problem escalation, problem management and notification). Service-level summary reports MUST be provided on request.	M	U
HST01.07	The EMR Vendor MUST maintain a current inventory of all information technology assets that comprise the hosted EMR Offering.	The information technology asset includes all technologies, owned or leased, within a logical (physical) or virtual (cloud-based) environment. The inventory of assets MUST include, but is not limited to: a) Type of asset b) Information technology owner c) Location of the information technology d) Backup and disaster recovery needs for applicable assets Backup and disaster recovery process for applicable assets	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST01.08	The EMR Vendor MUST document and maintain current logical network and integration architecture diagrams for the hosted EMR Offering, including all external connections and third-party integrations where applicable. Architecture documentation MUST be accompanied by a narrative description that explains network segmentation, trust boundaries, and connectivity to external systems.	The architecture documentation MUST include, at a minimum: a) Logical network segmentation and security zones b) Trust boundaries and ingress/egress points (firewalls network zones, DMZ, network zones) c) External connections, including integrations, including integration to Provincial EHR services d) Connectivity between application, database, storage, and supporting services e) Administrative and remote access pathways f) Dependencies on third-party service providers or cloud services Documentation MUST reflect the deployed architecture and be updated following material changes to the hosting environment.	M	U
HST01.09	The EMR vendor MUST identify and document the geographic location(s) where data associated with the EMR Offering is stored and processed.	The EMR vendor MUST provide a formal declaration identifying the geographic location(s) where EMR data is hosted and processed, including: a) Primary production region(s) b) Secondary / disaster recovery region(s) c) Any regions used by subcontractors, cloud service providers, or third-party infrastructure providers. The declaration MUST be supported by evidence, which may include: a) Cloud provider region configuration (e.g., AWS/Azure region configuration screenshots or documentation) b) Hosting architecture documentation identifying the configured region(s) c) Contractual documentation with the cloud or hosting provider specifying the geographic region d) Data residency controls demonstrating that data remains within the declared region(s)	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Where a public cloud provider is used, the vendor MUST identify the specific cloud regions and availability zones configured for the EMR environment.		
HST01.10	The EMR vendor MUST retain accountability for the confidentiality, integrity, and availability of the EMR Offering regardless of the use of third-party service providers.	The use of third-party infrastructure, cloud service providers, managed service providers, or subcontractors does not transfer or reduce the EMR vendor's responsibility for compliance with the requirements of this specification. The EMR vendor MUST ensure that all third-party providers supporting the EMR Offering operate in accordance with the applicable security, privacy, and hosting requirements defined in this specification. To demonstrate compliance, the EMR vendor MUST be prepared to provide documentation describing the shared responsibility model and governance of third-party providers, which MAY include: a) A security or operational shared responsibility matrix identifying responsibilities between the EMR vendor and any third-party service providers b) Documentation identifying third-party infrastructure providers, cloud services, or subcontractors used to support the EMR Offering c) Security assurance documentation such as ISO/IEC 27001 certification, SOC 2 reports d) Other equivalent third-party attestations	M	N
HST01.11	The EMR vendor MUST document the division of security and operational responsibilities.	The shared responsibility model shall identify vendor-managed and subscriber-managed controls, including access management, patch management, logging, backup, and configuration responsibilities.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST01.12	The EMR vendor MUST identify any third-party infrastructure or cloud service providers supporting the EMR Offering.	Identification MUST include provider name, service type (e.g., SaaS, IaaS, PaaS), and hosting region(s) used in production and backup systems.	M	N
HST01.13	The EMR vendor MUST maintain current assurance evidence for third-party infrastructure or cloud service providers supporting the EMR Offering.	Assurance evidence submitted MAY include current reports or certifications which follow recognized frameworks. Examples MAY include: a) SOC2 Type II audit reports b) ISO/IEC 27001 certification c) HITRUST r2 d) Other third-party audit reports or certifications determined by the organization which provide equivalent risk assurance	M	N

5. Security Controls

This section defines the technical safeguards applied within the hosting environment to protect systems and data from unauthorized access, misuse, and compromise.

5.1 Network and Infrastructure Safeguards

These requirements define security controls for network and system components, including segmentation, traffic control, and secure configuration, to protect EMR systems and data from unauthorized access and exposure.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST02.01	The EMR vendor MUST implement and maintain segregated network environments to isolate the hosted	Segregation may be logical or virtual in cloud-based deployments. Isolation shall apply across production, backup, and disaster recovery environments.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	EMR environment from external networks and unrelated systems.	Network segregation controls SHALL: a) Isolate production, backup, disaster recovery, and administrative networks b) Enforce network isolation between system tiers and prevent unauthorized lateral movement Prevent unauthorized lateral movement between system tiers c) Enforce least-privilege connectivity between services d) Apply logical, virtual, or physical segmentation appropriate to the deployment model e) Be reviewed periodically for effectiveness		
HST02.02	The EMR vendor MUST deploy and maintain all internal and external network perimeters to secure system boundaries of the hosted EMR environment.	Network boundary protection SHALL: a) Be implemented at all inbound and outbound trust boundaries, including external connections and internal security zones b) Enforce a default-deny posture with explicitly authorized traffic only c) Prevent unauthorized lateral movement between network segments d) Utilize appropriate boundary controls (e.g., firewalls, security groups, or equivalent cloud-native mechanisms) e) Be reviewed periodically to ensure continued alignment with the deployed architecture	M	U
HST02.03	The EMR vendor MUST configure all security gateways with a deny-all policy for both inbound and outbound traffic.	The EMR vendor implementation MUST fail-secure (fail-close) on critical connections where availability and need permits. In the event of a failure (e.g., system error, network disruption, or component outage), access to systems, data, or services is denied by default to prevent unauthorized access, rather than allowing continued or degraded access.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST02.04	The EMR vendor MUST implement a process to review security gateway configurations at least annually.	The review MUST be documented and approved by the designated Security Officer or other authorized party, to ensure the ongoing integrity of the configuration. The Process MUST ensure that: a) Review of the rule sets on their security gateways b) Removal of expired or unnecessary rules c) Resolution of conflicting rules d) Removal of unused or duplicate objects (e.g., network or computer systems)	M	U
HST02.05	The EMR vendor MUST ensure that authentication and authorization processes are in place on the hosted EMR Offering network before access to the hosted EMR Offering is granted.	The EMR vendor MUST ensure that no user, device, or executable process will be allowed to establish a connection without explicit verification or permission.	M	U
HST02.06	The EMR vendor MUST harden all information systems by disabling all non-essential services such as protocols and ports. Any service or port that remains active MUST have a documented technical justification, with a mapping to a specific system and system function.	System hardening controls MUST ensure that: a) only services, protocols, and network ports required for system operation are enabled b) any enabled service, protocol, or port has a documented technical justification linked to a specific system function c) system hardening configurations follow recognized security configuration standards or benchmarks where applicable d) system hardening configurations are reviewed periodically to ensure they remain consistent with security best practices Examples of recognized benchmarks may include: • Center for Internet Security (CIS) Benchmarks • NIST SP 800-123 or equivalent system hardening guidance	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST02.07	The EMR vendor MUST harden all information system components prior to implementation into the production environment.	The hosted EMR vendor MUST ensure that system components such as the operating system, databases, and applications, are hardened using a documented security standard or process prior to their deployment into a production environment.	M	U
HST02.08	The hosted EMR vendor MUST securely configure systems supporting the EMR Offering prior to production use by removing, disabling, or not enabling non-essential services, functions, and components.	The EMR Vendor MUST establish, document, implement, and maintain secure configuration standards for systems supporting the EMR Offering. These controls MUST ensure that: a) Only necessary services, functions, ports, protocols, software, and system components are enabled b) Non-essential components, including unused drivers, features, subsystems, file systems, and web servers, are removed, disabled, or otherwise rendered unavailable prior to production. c) Secure configuration practices are applied consistently across environments. d) For cloud-based environments, secure configuration is applied in accordance with the shared responsibility model and the nature of the cloud service used.	M	U
HST02.09	The hosted EMR vendor MUST ensure that services, protocols, and communication mechanisms used by systems supporting the EMR Offering are securely configured and protected against unauthorized access or interception.	The EMR vendor SHOULD ensure that secure communication protocols are used to protect data transmitted between system components, users, and external services. Where services or protocols that are considered insecure are required for compatibility or operational reasons, the EMR vendor SHOULD implement compensating security controls such as encryption or secure tunneling. Examples of secure protocols that may be used include: a) TLS for encrypted communications b) SSH or secure shell-based services	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) IPSec or equivalent network encryption mechanisms d) Secure file transfer mechanisms such as SFTP Insecure protocols or services (for example Telnet or FTP) SHOULD be disabled unless explicitly required and where enabled they SHOULD be protected through secure alternatives or encapsulated within encrypted channels. The EMR vendor SHOULD periodically review enabled services and protocols to ensure they remain aligned with current security best practices and cryptographic guidance.		
HST02.10	The EMR Vendor MUST harden intrusion detection and prevention sensors to prevent them from being identified, bypassed, or compromised.	Intrusion detection and prevention sensors MUST be hardened to protect their integrity and effectiveness. These controls MUST include: a) Restricting access to sensor devices and management interfaces to authorized personnel only b) Securing configuration settings to prevent unauthorized modification or disabling of sensors c) Protecting sensors from direct exposure to untrusted networks, except where required for their function d) Ensuring communications between sensors and management systems are secured e) Implementing measures to reduce the likelihood of sensors being identified or bypassed by unauthorized actors Where technically feasible, sensor configurations SHOULD operate in a fail-secure (fail-closed) manner. In the event of a failure or detected compromise, the sensor or associated control denies traffic or access by default to prevent unauthorized activity.	M	U
HST02.11	The EMR vendor or installed agent MUST scan inbound data for malware prior to the data being opened,	Malware scanning controls MUST include:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	executed, or processed by systems supporting the EMR Offering.	a) Scanning of inbound data from all relevant sources, including physical media, email attachments, file downloads, and data transfers b) Scanning performed prior to execution, access, or ingestion by the EMR Offering or user systems c) Implementation of malware scanning at appropriate control points within the environment (e.g., email gateways, network boundaries, and endpoint devices) Malware scanning MAY be performed at multiple layers to provide defense-in-depth (e.g., email servers, network controls, and endpoint systems).		

5.2 Identity and Access Controls

These requirements define controls for managing identities and access to the hosting environment, including vendor personnel, administrative and service accounts, and remote access, complementing the Privacy and Security requirements.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST05.04	The vendor MUST ensure that all access is provisioned based on the requestor's established business needs, in accordance with their privacy policies, and in accordance with the principles of need-to-know and least-privilege (e.g., an agent or electronic service provider is granted only the minimum access privileges required). The vendor is responsible for identifying all their agents	Access provisioning controls MUST include: a) assignment of access rights based on defined roles or responsibilities b) validation that access requests align with documented business need c) limitation of access to only those systems and functions required to perform assigned duties d) identification and tracking of all vendor personnel, agents, and service providers requiring access	M	R

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	and electronic service providers who require access to the hosted EMR Vendor.			
HST03.01	The vendor MUST implement access control mechanisms for the hosted EMR environment that support authentication and authorization.	Access control mechanisms MUST: a) uniquely identify and authenticate users and systems b) enforce authorization decisions based on assigned permissions c) restrict access to system resources, data, and services based on defined access policies	M	U
HST03.02	The vendor MUST ensure that access to and use of the hosted EMR environment is traceable to a unique user or system identity.	Traceability controls MUST ensure that: a) user activities are attributable to a single individual b) service account activity is attributable to a specific system and owner c) audit logs support identification of the initiating identity	M	U
HST05.08	The vendor MUST configure its access control and identity management system to deny access by default to the hosted EMR Vendor.	Default-deny controls MUST ensure that: a) access is granted only through explicit authorization b) unauthorized access attempts are denied by default c) access rules are reviewed periodically	M	R
HST03.03	The vendor MUST require the creation or amendment of an ID managed by the vendor to be initiated by a written or electronic request (e.g., via an email or help desk ticket) that is approved by an authorized representative of the subscriber (the requestor) unless the ID is created through an automated process (e.g., a Service ID during the installation of software).	The request for ID creation MUST contain the access privileges requested and may contain the following information: a) details of the authorized requestor: full name, department, sponsor authority, location, and contact information (email and telephone number (where available)) b) details of whom the ID is to be assigned to: full name, department, location, and contact information (email and telephone number (where available)) or in the case of a Service ID, details of the information system on which the ID is being created and owner	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) justification for the request (if applicable, e.g., when requesting a Privileged ID)		
HST03.04	The vendor MUST maintain a list of all identities that have access to the hosted EMR Vendor.	The list MUST include the following: a) identity (user or system ID) b) Person or information system's details: Full name, department, location, and contact information (email and telephone (where applicable)) c) Privileges associated with the ID d) Requirement/function (for Service IDs only) e) Applicable service account relationships and interactions (for Service IDs only)	M	U
HST03.05	The EMR Vendor MUST ensure that privileged account names do not indicate their privilege level.	Controls MUST ensure that: a) naming conventions do not expose elevated access b) privileged accounts are not easily identifiable	M	U
HST03.06	The EMR Vendor MUST ensure that privileged access is assigned to separate accounts from standard user accounts.	Controls MUST ensure that privileged and non-privileged activities are separated users operate under standard accounts for routine activities.	M	U
HST03.07	The vendor MUST ensure that the assignment and use of Privileged IDs are limited to the minimum number of persons who are directly responsible for operational support or administration.	Controls MUST ensure that: a) privileged access is restricted to authorized personnel b) access is granted based on operational necessity c) privileged access is limited to the minimum number of individuals required (principle of least privilege) d) the scope of privileged access is appropriate to the deployment model	M	U
HST03.08	The EMR Vendor MUST ensure that service account naming conventions are standardized and do not expose	Service account naming controls MUST ensure that: a) naming conventions are consistent and documented	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	system dependencies or underlying infrastructure details.	b) names do not reveal system architecture, hostnames, or sensitive implementation details c) service accounts can be uniquely identified and linked to their purpose		
HST03.09	The vendor MUST ensure that Service IDs are not capable of interactive sign-on.	Controls MUST ensure that: a) interactive login capabilities are disabled for service accounts b) service accounts are restricted to system-to-system or automated processes c) authentication methods for service accounts are limited to approved mechanisms	M	U
HST03.10	The vendor MUST ensure that an identified owner is assigned to each Service ID.	Service account management MUST ensure that: a) each service account has a designated accountable owner b) ownership information is documented and maintained c) owners are responsible for reviewing usage and access requirements	M	U
HST05.21	The EMR Vendor MUST ensure that credentials used by non-interactive service accounts are managed securely in accordance with defined credential management practices.	Credential management controls MUST ensure that: a) credentials are protected using secure storage mechanisms (e.g., vaulting or equivalent) b) use of non-expiring credentials is limited to cases where technically required c) compensating controls are implemented where credentials cannot be rotated (e.g., monitoring, restricted scope) d) credential usage is auditable	M	R
HST03.11	The EMR Vendor MUST ensure that service account credentials are changed under defined conditions.	Credential lifecycle controls MUST ensure that: a) credentials are changed following suspected or confirmed compromise	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) credentials are updated when personnel with knowledge of the credential leave or change roles c) credentials are updated when system or technology changes occur d) automated or periodic rotation is implemented where technically feasible		
HST03.12	The vendor MUST ensure that authentication mechanisms used for system-to-system or API communications uniquely identify the calling system or service and are not shared across multiple entities.	Controls MUST ensure that: a) non-interactive authentication mechanisms (e.g., certificates, tokens, client credentials) are uniquely assigned to a specific system or service b) shared use of authentication credentials across multiple systems or services is prohibited c) authentication credentials are traceable to a specific system, service, and accountable owner d) concurrent or anomalous use of the same credential across multiple systems is prevented or detected e) authentication mechanisms align with approved standards and protocols (e.g., OAuth2, mTLS, signed tokens)	M	U
HST05.27	The vendor MUST ensure that their information systems are technically capable of accepting all passwords that meet the requirements and ensure compliance with the account lockout, lockout duration, history and minimum age requirements for passwords used to access the hosted EMR Offering. See 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.	Password enforcement controls MUST ensure that: a) systems enforce defined password complexity and policy requirements b) account lockout, history, and aging controls are applied consistently c) password validation mechanisms accept compliant passwords without restriction d) enforcement aligns with Appendix B requirements	M	R

OMD #	REQUIREMENT		GUIDELINES	M/O	STATUS						
	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.										
		<table><tr><th></th><th>Personal IDs & Privileged IDs</th><th>Service IDs</th></tr><tr><td>Length</td><td>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.</td><td>Be at least 15 characters and randomly generated where possible.</td></tr></table>		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.			
	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.									

OMD #	REQUIREMENT			GUIDELINES	M/O	STATUS
	C o m p l e x i t y	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).			

	A d d i t i o n a l P a s s w o r d A t t r i b u t e s	- 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,	Service credentials MUST be protected using secure credential storage mechanisms. Hard-coded credentials MUST NOT be stored in applications, scripts, or configuration files			
--	--	--	---	--	--	--

OMD #	REQUIREMENT			GUIDELINES	M/O	STATUS
		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.				
	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.			

OMD #	REQUIREMENT		GUIDELINES	M/O	STATUS
	A c c o u n t L o c k o u t	Authentication systems MUST implement protections against repeated failed login attempts (e.g., lockout thresholds or rate limiting).			
	L o c k o u t d u r a t i o n	Until manually unlocked by: • An administrator, or • A self-service password reset facility. – OR – Unlocked after a minimum of 30 minutes			

OMD #	REQUIREMENT		GUIDELINES	M/O	STATUS
	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. for more information.				
HST03.13	The vendor MUST display a terms-of-use (ToS) banner or message at, or prior to, initial user authentication. The terms of use MUST be accepted by the EMR user in order to gain access to the hosted EMR Offering.		Acceptable use controls MUST ensure that: a) users are presented with a terms-of-use message prior to authentication b) access is granted only after explicit acknowledgment of the terms c) terms define acceptable use, responsibilities, and legal obligations	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		d) acknowledgment of terms is recorded or enforced by the system		
HST03.14	In the event of an authentication failure (e.g., an invalid sign-on attempt), the vendor MUST ensure that the hosted EMR Offering does not indicate the reason for the failure (e.g., state that it was an incorrect password or that the ID does not exist on the system).	Authentication response controls MUST ensure that: a) authentication failure messages do not reveal whether the username or password is incorrect b) responses do not disclose account existence or system details c) authentication mechanisms prevent user enumeration attacks d) error handling is consistent across authentication scenarios	M	U
HST03.15	The vendor MUST secure all default IDs (commonly known as vendor IDs).	Controls MUST ensure that: a) default or vendor-supplied accounts are disabled, removed, or renamed prior to production use b) any retained accounts are secured and monitored c) default credentials are not used in any environment beyond initial setup	M	U
HST03.16	The vendor MUST change or set all default passwords, including null passwords, prior to deployment in a production environment and as soon as reasonably possible in a non-production environment.	Controls MUST ensure that: a) all default or null passwords are changed prior to system deployment b) default passwords are not reused across environments c) systems are validated prior to production to confirm no default credentials remain	M	U
HST05.39	The EMR Vendor MUST enforce multi-factor authentication for remote access to the hosted EMR environment.	Remote access controls MUST ensure that: a) MFA is required for all remote access connections, including administrative access b) authentication controls for passwords and authenticators align with Appendix B: Minimum Password Requirements	M	R

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) MFA is enforced for access from untrusted or external networks		
HST03.17	The EMR Vendor MUST restrict privileged remote access to approved secure access mechanisms.	Remote access controls MUST ensure that: a) privileged access is performed through approved secure access solutions (e.g., virtual workspace, jump host, or equivalent) b) direct access to production systems is restricted where feasible c) remote access pathways are documented and controlled	M	U
HST03.18	The EMR Vendor MUST maintain a record of all authorized administrative remote access.	The record MUST include: a) user or system identity b) associated individual details c) date of access provisioning d) level of access granted e) approving authority The inventory MUST be periodically reviewed to ensure continued validity of access.	M	U
HST03.19	The vendor MUST employ cryptographic solutions to maintain session confidentiality and integrity of all remote access connections.	Session protection controls MUST ensure that: a) remote sessions are protected using cryptographic mechanisms in accordance with Appendix D: Approved Cryptographic Algorithms b) session integrity is protected against interception or tampering c) session configurations align with organizational cryptographic standards	M	U
HST03.20	The EMR vendor MUST restrict and control access to system documentation and operating procedures based on the principles of least privilege and need-to-know.	The access to documentation SHOULD be role based (RBAC) and limited to specific job functions. Such examples MAY include: a) Senior Operations with access to recovery keys	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) Support Staff with views limited to troubleshooting guides		
HST03.21	The vendor MUST assign all their employees, agents, electronic service providers, and information systems a unique ID before provisioning them with access to the hosted EMR Vendor.	Unique identification controls MUST ensure that: a) each identifier is assigned to a single individual or system b) shared or generic user IDs are not permitted, except for approved service accounts c) identifiers support traceability and accountability	M	U
HST03.22	The EMR vendor MUST maintain a log of all requests for IDs that it manages and that could be used to access the hosted EMR Vendor.	Records MUST include: a) request details and requested access b) approval information c) date of request and implementation d) associated user or system identity	M	U
HST03.23	The EMR Vendor MUST periodically review access rights to ensure continued appropriateness.	Access review processes MUST ensure that: a) access rights are reviewed at least annually b) inappropriate or excessive access is modified or revoked c) review outcomes are documented	M	U
HST03.24	The EMR Vendor MUST ensure that access rights are modified or revoked upon changes in employment status or role.	Deprovisioning controls MUST ensure that: a) access is removed or adjusted promptly upon termination or role change b) privileged access is revoked immediately where applicable c) changes are documented	M	U
HST03.25	The vendor MUST communicate initial passwords or passphrases ("passwords") securely. Where an ID has been communicated through email, the associated	Credential distribution controls MUST ensure that: a) initial passwords are communicated using secure transmission methods	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	password MUST be communicated through an alternative communication channel (e.g., via phone).	b) separate communication channels are used for IDs and passwords where feasible c) exposure of credentials during transmission is minimized d) credential delivery processes are documented and controlled		
HST03.26	The vendor MUST set initial passwords to prompt the EMR user to change their password at initial login or MUST ensure that the EMR user is manually instructed to change their password at initial login.	Credential initialization controls MUST ensure that: a) users are required to change initial passwords upon first authentication b) temporary credentials are not usable beyond initial login c) initial password change requirements are enforced by system controls or formal procedures	M	U
HST03.27	The EMR Offering MUST ensure that all passwords are masked or concealed on entry, i.e., represented on the screen by a special character such as an asterisk.	Password entry protection controls MUST ensure that: a) passwords are masked during entry to prevent observation b) display mechanisms prevent exposure of sensitive authentication data c) user interfaces are designed to reduce risk of credential disclosure	M	U
HST03.28	The vendor MUST only reset a password after the EMR user's identity has been successfully verified.	Password reset controls MUST ensure that: a) user identity is verified prior to password reset b) verification methods follow defined authentication procedures c) reset actions are documented and auditable d) unauthorized password reset attempts are prevented	M	U
HST03.29	The EMR Offering MUST encrypt passwords in transmission.	Password transmission controls MUST ensure that: a) passwords are encrypted during transmission using approved protocols	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) insecure transmission methods are not permitted c) authentication exchanges are protected from interception		
HST03.30	The vendor MUST protect passwords in storage. Where passwords stored in files cannot be encrypted, passwords MUST not indicate the information system or ID for which they are associated.	Password storage controls MUST ensure that: a) passwords are protected using secure hashing or encryption mechanisms in accordance with approved cryptographic standards b) stored credentials are not retrievable in clear text by users or administrators c) access to stored credentials is restricted to authorized system processes d) storage mechanisms prevent association of passwords with identifiable systems or user IDs where encryption is not feasible	M	U
HST03.31	The vendor MUST not cache unencrypted passwords.	Credential caching controls MUST ensure that: a) unencrypted passwords are not stored in memory, cache, or temporary storage locations b) cached authentication data is protected using secure mechanisms where caching is required c) systems prevent reuse or exposure of cached credentials d) credential storage in memory is minimized and controlled	M	U
HST03.32	The vendor MUST not hard-code clear text passwords in information systems or stored in batch files or scripts.	Secure coding controls MUST ensure that: a) passwords are not embedded in application code, configuration files, scripts, or batch processes b) secure credential storage mechanisms are used in place of hard-coded values c) access to credentials is restricted and auditable d) development practices prevent introduction of embedded credentials	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST03.33	The vendor MUST ensure that clear-text passwords are not embedded in any automated login process or stored in a macro, script or function key.	Automated authentication controls MUST ensure that: a) clear-text passwords are not stored in automation tools, macros, scripts, or function keys b) secure authentication mechanisms are used for automated processes c) credentials used in automation are protected using secure storage or vaulting mechanisms d) exposure of credentials through automation processes is prevented	M	U
HST03.34	The vendor MUST ensure that all paper-based passwords used for backup or contingency purposes are stored using the principle of dual control or split knowledge.	Contingency credential handling controls MUST ensure that: a) paper-based or backup credentials are protected using dual control or split knowledge principles b) access to physical credentials is restricted to authorized personnel c) storage locations for such credentials are secured against unauthorized access d) access and use of contingency credentials are logged and controlled	M	U
HST03.35	The EMR Vendor MUST 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	U

5.3 Cryptography

The following section describes the implementation requirements for cryptographic algorithms, the protection of data through encryption, and the management of the underlying key lifecycle. Appendix D: Approved Cryptographic Algorithms support these requirements.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST04.01	The EMR vendor MUST encrypt all PHI while in transit across any internal or external network.	The EMR Vendor MUST ensure that the encryption used provides end-to-end protection for both Confidentiality (preventing unauthorized viewing) and Integrity (preventing unauthorized modification) of the data.	M	U
HST04.02	The EMR vendor MUST implement full disk or partial disk encryption on any mobile workstation (e.g. laptops, etc.) that stores PHI.	The EMR vendor MUST consider full-disk encryption as a best practice using AES-256bit encryption as a standard to protect data at rest.	M	U
HST04.03	The EMR vendor MUST encrypt all data classified as internal or higher, inclusive of PHI, before it is stored on any device (E.g. hard drive, removeable media, backup tape) that will be sent externally.	The EMR vendor MUST ensure that the removal of information classified as confidential or higher will be done so that the information cannot be recovered and viewed by unauthorized individuals.	M	U
HST04.04	The EMR vendor MUST ensure that the hosted EMR Vendor use only approved cryptographic algorithms.	The EMR vendor MUST implement cryptographic algorithms, protocols, and key lengths in accordance with Appendix D: Approved Cryptographic Algorithms. This includes, as applicable: a) Encryption algorithms for data at rest b) Protocols for data in transit (e.g., TLS1.2+) c) Hashing and integrity mechanisms d) Key establishment, key transport, and digital certificate standards	M	U
HST04.05	The EMR vendor MUST ensure that every proposed implementation of a cryptographic solution within the hosted EMR Vendor undergoes a formal assessment by a qualified information security specialist.	The EMR vendor MUST ensure cryptographic implementations are reviewed prior to production deployment to confirm they meet security and compliance expectations. The assessment MUST include, as applicable: a) Algorithm/protocol selection aligned with Appendix D: Approved Cryptographic Algorithms b) Key management approach and storage location(s) c) Integration design (applications, infrastructure, third parties) d) Failure modes and operational impacts	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST04.06	The EMR vendor MUST configure all cryptographic solutions to fail-close in the event of a failure within the encryption or decryption process.	The EMR vendor MUST ensure cryptographic failures result in a secure default state. Controls MUST include, as applicable: a) Denying access when encryption/decryption or validation fails b) Preventing bypass of encryption, integrity, or authentication controls c) Logging and alerting on cryptographic failures	M	U
HST04.07	The EMR vendor MUST document and formalize contingency procedures for all cryptographic implementations prior to their deployment in a production environment.	The EMR vendor MUST ensure cryptographic failures result in a secure default state. Controls MUST include, as applicable: a) Denying access when encryption/decryption or validation fails b) Preventing bypass of encryption, integrity, or authentication controls c) Logging and alerting on cryptographic failures	M	U
HST04.08	The EMR vendor MUST utilize hardware-based cryptography rather than software only cryptographic solutions in environments that store or process PHI.	The EMR vendor MUST ensure cryptographic keys for PHI are protected using hardware-backed controls appropriate to the hosting model. Hardware-backed controls MUST include, as applicable: a) Dedicated HSMs or managed HSM/KMS services b) Logical isolation of key material from general-purpose compute c) Administrative access restrictions and monitoring of key operations	M	U
HST04.09	Where cryptographic hardware devices are used, The EMR Vendor MUST ensure that these devices meet or exceed the tamper-resistant enclosure requirements specified in the Federal Information Processing Standards (FIPS) 140-2 Level 3 standard.	The EMR vendor MUST ensure cryptographic modules used for PHI meet applicable assurance levels. Controls MUST include, as applicable: a) Certification evidence for the module/service (e.g., FIPS validation) b) Configuration consistent with the certified operating mode c) Physical/logical protections aligned to the module deployment model	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST04.10	The EMR Vendor MUST restrict the use of software-based cryptographic solutions to approved use cases, including one-way cryptographic functions, secure remote access, client-side storage encryption, digital certificate processing, and data encryption where hardware-based cryptographic controls are not required.	Software-based cryptographic implementations MUST only be used for the following purposes: a) one-way or non-reversible cryptographic functions such as hashing b) client-side software supporting secure remote access connections c) client-side storage encryption including full-disk encryption d) digital certificate processing or management on client-side or server-side systems e) encryption of data stored within data centres where hardware cryptographic modules are not required Software cryptographic implementations MUST utilize industry-recognized cryptographic libraries and algorithms that comply with the EMR vendor's approved cryptographic standards. Where cryptographic mechanisms protect highly sensitive data or critical infrastructure components, the EMR vendor MUST ensure that appropriate cryptographic controls are implemented and managed in accordance with documented cryptographic policies.	M	U
HST04.11	Where software-based cryptographic mechanisms are implemented, the EMR Vendor MUST ensure that cryptographic keys, passwords, or other authentication secrets are not stored in application code, program files, batch files, or script files.	Cryptographic secrets MUST be protected using secure storage mechanisms and access controls. Secret protection mechanisms MUST ensure that: a) passwords, cryptographic keys, or authentication secrets are not embedded in application source code, configuration scripts, or automation files b) secrets used for system operation are stored in protected configuration stores, secure credential vaults, or equivalent secure secret management systems	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) access to files or systems containing cryptographic secrets is restricted to authorized processes or administrative users d) cryptographic material associated with digital certificates or server authentication mechanisms is protected using appropriate file permissions or secure storage mechanisms Where server-based digital certificates require passphrases or protected key files, access to those files MUST be restricted through appropriate access control mechanisms.		
HST04.12	The EMR Offering MUST protect cryptographic keys, including secret and private keys, from unauthorized access, disclosure, modification, loss, or destruction.	Cryptographic key protection mechanisms MUST ensure that: a) cryptographic keys are stored in secure locations using protected storage mechanisms such as hardware security modules, secure key stores, or equivalent key management systems b) access to cryptographic keys is restricted to authorized processes and administrative users c) cryptographic keys used by Internet-facing systems are protected from unauthorized disclosure or modification d) systems or equipment used to generate, load, store, or archive cryptographic keys are protected from unauthorized physical access or tampering e) cryptographic keys are managed in accordance with documented key management procedures including generation, storage, rotation, backup, and revocation	M	U
HST04.13	The EMR Vendor MUST ensure that MAC values are appended to the data from which it is calculated.	Message integrity controls MUST ensure that: a) message authentication codes (MAC) are generated and appended to data to verify integrity and authenticity b) MAC generation uses approved cryptographic algorithms and key management practices	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) MAC values are validated upon receipt prior to processing data d) integrity validation failures are detected and handled securely		
HST04.14	The EMR Vendor MUST ensure that all hash functions are one-way (i.e., non-reversible).	Hashing controls MUST ensure that: a) hash functions are one-way and non-reversible b) approved cryptographic hash algorithms are used c) hashing mechanisms protect against collision and preimage attacks d) hash outputs are used only for integrity verification or secure storage purposes	M	U
HST04.15	The EMR Vendor MUST only use a digital signature for the purpose of signing.	Digital signature controls MUST ensure that: a) digital signatures are used solely for authentication, integrity, and non-repudiation purposes b) signing keys are protected and used only for authorized signing operations c) signature generation and verification use approved cryptographic standards d) signature validation occurs prior to trusting signed data	M	U
HST04.16	The EMR Vendor MUST ensure that all digital certificates are revocable.	Certificate lifecycle controls MUST ensure that: a) digital certificates support revocation mechanisms b) certificate status is validated prior to trust decisions c) expired or revoked certificates are not accepted d) certificate lifecycle management processes are defined and maintained	M	U
HST04.17	The EMR Vendor MUST implement digital certificates with a cryptographically secured Certificate Revocation List (CRL) system.	Certificate revocation controls MUST ensure that: a) CRL or equivalent mechanisms are implemented and maintained b) CRLs are cryptographically protected and validated prior to use	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) revocation information is updated and distributed in a timely manner d) systems check revocation status prior to trusting certificates		
HST04.18	The EMR Vendor MUST ensure that a digital certificate is only trusted once it has been cryptographically validated and does not appear on a trusted CRL.	Certificate validation controls MUST ensure that: a) digital certificates are validated using trusted certificate authorities b) certificate chains are verified prior to trust c) revocation status is checked using CRL or equivalent mechanisms d) only valid and trusted certificates are accepted for use	M	U
HST04.19	The EMR Vendor MUST protect its cryptographic keys against unauthorized access (in the case of secret and private keys), modification, loss, and accidental or intentional destruction.	Cryptographic key protection controls MUST ensure that: a) cryptographic keys are protected from unauthorized access, modification, or disclosure b) key storage mechanisms use secure and approved protection methods c) key lifecycle events are managed in accordance with defined procedures d) key compromise risks are mitigated through monitoring and controls	M	U
HST04.20	The EMR Vendor MUST ensure that equipment used to generate, load, store and archive cryptographic keys is physically protected against unauthorized access or modification.	Key management infrastructure controls MUST ensure that: a) systems used for key generation, storage, and processing are physically secured b) access to key management systems is restricted to authorized personnel c) physical and environmental protections prevent unauthorized access or tampering d) key management environments are monitored and controlled	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST04.21	The EMR Vendor MUST establish and maintain documented processes for managing cryptographic keys used within the EMR Offering.	Cryptographic key management processes MUST include procedures for: a) the secure generation, distribution, loading, storage, recovery, replacement, revocation, and destruction of cryptographic keys b) the secure backup and archival of cryptographic keys where required for system operation c) restricting access to cryptographic keys to authorized personnel or system processes d) protecting cryptographic keys throughout their lifecycle in accordance with approved cryptographic standards	M	U
HST04.22	The EMR Vendor MUST maintain and protect a comprehensive inventory of all cryptographic keys and key components to support traceability, accountability, and lifecycle management.	The cryptographic key inventory MUST be maintained to support traceability and lifecycle management of cryptographic keys and MUST include, where applicable: a) the key identifier, name, and intended purpose or usage b) the cryptographic key type (e.g., symmetric, private key, public key) c) the date of key generation and activation d) the storage location or key management system where the key is maintained e) the identity of authorized custodians or systems responsible for managing the key f) the lifecycle status of the key, including activation, rotation, revocation, or destruction g) records of key destruction or retirement where applicable The cryptographic key inventory MUST be protected from unauthorized access or modification and MUST be maintained in accordance with the EMR Vendor's key management processes.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST04.23	The EMR Vendor MUST review the inventory of its cryptographic keys annually.	Key inventory review controls MUST ensure that: a) the cryptographic key inventory is reviewed at least annually to confirm accuracy and completeness b) key records reflect current lifecycle status, including active, rotated, revoked, or retired keys c) discrepancies or unauthorized entries are identified and investigated d) outdated or unused keys are identified for rotation or removal in accordance with key management processes e) review outcomes are documented and retained for audit purposes	M	U
HST04.24	The EMR Vendor MUST maintain and protect logs of cryptographic key lifecycle events, including generation, access, use, storage, and destruction, to ensure traceability and accountability.	Key lifecycle logging controls MUST ensure that: a) key generation or creation events are recorded b) key activation, rotation, or revocation events are recorded c) key access or use is recorded where applicable d) key archival or destruction events are recorded e) logs are protected from unauthorized modification f) logs are retained in accordance with the EMR Vendor's security logging policies.	M	U
HST09.22	The EMR Vendor MUST review the audit logs of its keys annually.		M	R
HST09.23	The EMR Vendor MUST restrict access to secret keys or key components, key devices and key materials to key custodians and their backups. Generally, the designation of a primary and a backup key custodian for each key or key component is sufficient.		M	R

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST09.24	The EMR Vendor MUST store keys in the fewest possible locations and forms.		M	R
HST04.25	The EMR Vendor MUST ensure that backup copies of secret keys are created only for the purpose of recovering keys that are lost, destroyed, or otherwise inaccessible.	Cryptographic key backup mechanisms MUST ensure that: a) backup copies of cryptographic keys are created only where required to support key recovery or system continuity b) backup keys are stored using approved secure storage mechanisms consistent with the storage requirements for the original key c) access to backup keys is restricted to authorized personnel or systems responsible for key management d) backup keys are protected from unauthorized access, modification, or disclosure e) the lifecycle of backup keys is managed in accordance with the EMR Vendor's cryptographic key management procedures	M	U
HST04.26	The EMR Vendor MUST ensure that the backup copies of secret keys are stored with strict access controls, under dual control, and subject to at least the same level of control as operational keys.	Protection mechanisms for backup cryptographic keys MUST ensure that: a) access to backup keys is restricted to authorized personnel or system processes responsible for key management b) backup keys are protected using access control and security mechanisms equivalent to or stronger than those applied to operational keys c) appropriate separation of duties or multi-party authorization controls are implemented where required for key management operations d) backup keys are protected from unauthorized disclosure, modification, or loss	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST04.27	The EMR Vendor MUST ensure that the creation of backup copies (including cloning) requires at least two authorized persons to enable the process. All requirements applicable for the original keys MUST also apply to any backup copies of keys and their components.	Protection mechanisms for backup cryptographic keys MUST ensure that: a) access to backup keys is restricted to authorized personnel or system processes responsible for key management b) backup keys are protected using access control and security mechanisms equivalent to or stronger than those applied to operational keys c) appropriate separation of duties or multi-party authorization controls are implemented where required for key management operations d) backup keys are protected from unauthorized disclosure, modification, or loss	M	U
HST04.28	The EMR Vendor MUST ensure that cryptographic keys that are no longer required, have been replaced, or have reached the end of their lifecycle are securely revoked and destroyed.	Cryptographic key revocation and destruction processes MUST ensure that: a) cryptographic keys that are expired, compromised, or no longer required are promptly revoked or deactivated b) replaced or retired keys are securely destroyed or rendered unusable c) destruction of cryptographic keys prevents reconstruction or recovery of the key material d) revocation and destruction events are recorded in accordance with the EMR Vendor's key management procedures	M	U
HST04.29	The EMR Vendor MUST ensure that cryptographic key generation is performed only by authorized personnel or approved system processes in accordance with documented key management procedures.	Cryptographic key generation mechanisms MUST ensure that: a) key generation activities are restricted to authorized individuals, roles, or system processes b) cryptographic keys are generated using approved cryptographic algorithms and secure generation mechanisms	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) key generation events are recorded in accordance with key management logging procedures d) automated key generation processes are governed by the EMR Vendor's key management policies		
HST04.30	The EMR Vendor MUST ensure that all keys and key components are generated using a random number generator or a pseudo-random number generator that passes all the basic tests for statistical randomness.	Cryptographic key generation mechanisms MUST ensure that: a) cryptographic keys are generated using Cryptographically Secure Random Number Generators (CSPRNGs) b) random number generation mechanisms are implemented using approved cryptographic libraries, hardware security modules, or equivalent trusted cryptographic services c) the random number generation mechanisms comply with recognized cryptographic standards and industry best practices	M	U
HST04.31	The EMR Vendor MUST ensure that secret keys are protected using secure storage and access control mechanisms that prevent unauthorized disclosure, duplication, or misuse.	Secret key protection mechanisms MUST ensure that: a) secret keys are stored using secure cryptographic storage mechanisms such as hardware security modules, secure key stores, or equivalent trusted key management systems b) secret keys are protected using encryption or equivalent safeguards when stored outside protected cryptographic modules c) access to secret keys is restricted to authorized personnel or system processes responsible for key management d) appropriate safeguards such as separation of duties, role-based access control, or multi-party authorization are implemented where required for key management operations	M	U
HST09.32	The EMR Vendor MUST ensure that the output of the key generation process is monitored by at least two authorized agents or electronic service providers.		M	R

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST04.32	The EMR Vendor MUST ensure that multi-use or multi-purpose computing systems are not used for key generation where any clear-text secret key or key component thereof appears in unprotected memory.	Key generation mechanisms MUST ensure that: a) secret keys are generated within protected cryptographic modules or secure key management systems where possible b) secret keys are not exposed in clear text outside protected memory regions of cryptographic modules or trusted cryptographic libraries c) key generation processes use secure cryptographic modules, hardware security modules, or equivalent trusted cryptographic services where available d) systems performing key generation implement appropriate protections to prevent unauthorized access to memory containing cryptographic key material	M	U
HST04.33	The EMR Vendor MUST ensure that a Key Encryption Key (KEK) is transferred by physically forwarding the separate components of the key using different communication channels or is transmitted electronically in ciphertext form.	Key transfer mechanisms MUST ensure that: a) cryptographic keys are transferred in encrypted form using approved cryptographic protocols or key-wrapping mechanisms b) secure communication channels are used when transmitting keys electronically c) key transfer processes are restricted to authorized personnel or system processes d) appropriate safeguards such as separation of duties or multi-party authorization are implemented where manual key transfer procedures are used	M	U
HST04.34	The EMR Vendor MUST ensure that any sign of package tampering results in the destruction and replacement of the set of key components, as well as any keys encrypted under this (combined) key.	Key compromise response procedures MUST ensure that: a) suspected or confirmed compromise of cryptographic key material results in immediate revocation or deactivation of the affected key	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) affected cryptographic keys are securely destroyed or rendered unusable c) new cryptographic keys are generated and distributed using approved key management procedures d) systems or data protected by compromised keys are re-secured using replacement keys where required		
HST04.35	The EMR Vendor MUST ensure that mechanisms exist to ensure that only authorized key custodians place key components into tamper-evident packaging for transmittal and that only authorized key custodians open tamper-evident packaging containing key components upon receipt.	Key distribution mechanisms MUST ensure that: a) only authorized individuals, roles, or system processes can perform cryptographic key distribution or import operations b) key distribution activities are logged and auditable c) secure cryptographic protocols or key-wrapping mechanisms are used when transferring keys electronically d) appropriate safeguards such as separation of duties or role-based authorization are implemented where manual key handling procedures are required	M	U
HST04.36	The EMR Vendor MUST ensure that keys or key components are never loaded (or reloaded) when there is any suspicion that either the key, key components or the cryptographic device has been compromised.	Key compromise response procedures MUST ensure that: a) cryptographic keys suspected of compromise are immediately revoked or disabled b) compromised or suspected compromised keys are securely destroyed or replaced c) affected cryptographic systems are re-secured using newly generated keys d) incidents involving potential key compromise are handled in accordance with the EMR Vendor's security incident response procedures	M	U
HST04.37	The EMR Vendor MUST ensure that unencrypted secret keys are entered into cryptographic devices using the principles of dual control and split	Key loading and import controls MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	knowledge. In instances where a secure key-loading device is used, only dual control is required.	a) cryptographic key loading or import operations are restricted to authorized personnel, roles, or approved system processes b) separation of duties or role-based access controls are implemented for manual key management activities c) secure key loading mechanisms or key management systems are used when provisioning cryptographic keys		
HST04.38	The EMR Vendor MUST ensure that any hardware used in the key-loading function is controlled and maintained in a secure environment under dual control.	Cryptographic key management systems MUST ensure that: a) systems used to manage or provision cryptographic keys operate within secured and access-controlled environments b) administrative access to key management systems is restricted to authorized personnel or system roles c) access to key management hardware or systems is monitored and logged	M	U
HST04.39	The EMR Vendor MUST require key custodians to examine all cable attachments before each key loading activity to ensure they have not been tampered with or compromised.	Key management integrity controls MUST ensure that: a) systems used for cryptographic key loading or management implement controls to detect unauthorized modification or tampering b) interfaces and connections used during key management operations are verified prior to performing key loading activities c) monitoring and logging mechanisms exist for key management operations	M	U
HST04.40	The EMR Vendor MUST define and implement procedures to prevent or detect the unauthorized substitution (unauthorized key replacement and key	Cryptographic key integrity controls MUST ensure that: a) mechanisms exist to prevent unauthorized substitution, misuse, or replacement of cryptographic keys	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	misuse) of one key or key component for another, or the operation of any cryptographic device without legitimate keys or key components.	b) key management systems validate keys and ensure they correspond to their intended cryptographic purpose c) access to cryptographic devices or key management systems requires authorized credentials or cryptographic keys		
HST04.41	The EMR Vendor MUST ensure that cryptographic keys are only used for a single intended purpose and MUST never be shared between production and non-production environments.	Cryptographic key usage controls MUST ensure that: a) cryptographic keys are assigned a single intended purpose and are not reused for different cryptographic functions b) cryptographic keys used in production environments are logically separated from those used in development or testing environments c) controls prevent the use of non-production keys in production systems	M	U
HST04.42	The EMR Vendor MUST ensure that all secret keys used for any function are unique (except by chance) to that device.	Cryptographic key generation controls MUST ensure that: a) cryptographic keys are generated to ensure uniqueness and prevent unintended reuse across devices or systems b) key generation processes use secure random generation mechanisms consistent with approved cryptographic standards c) systems prevent duplication or reuse of secret keys unless explicitly authorized by key management procedures	M	U
HST04.43	Digital certificates MUST have defined validity periods and be managed in accordance with approved cryptographic standards and risk-based practices.	Certificate lifecycle management MUST ensure that: a) Certificate validity periods are defined based on risk, usage, and exposure b) Certificates are rotated or renewed prior to expiration c) Certificate lifespans are minimized to reduce the risk of key compromise d) Public-facing certificates align with industry requirements (e.g., ≤ 398 days)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		e) Certificate revocation mechanisms (e.g., CRL, OCSP) are implemented and enforce		
HST04.44	The EMR Vendor MUST ensure that an uncompromised key is replaced on or before its stipulated lifespan.	Cryptographic key lifecycle management MUST ensure that: a) cryptographic keys are rotated or replaced prior to reaching their defined maximum lifespan b) automated or managed key rotation mechanisms are used where feasible c) systems prevent the continued use of expired cryptographic keys	M	U
HST04.45	The EMR Vendor MUST ensure that cryptographic keys that are compromised or suspected of compromise are promptly revoked and replaced in accordance with documented key management procedures.	Cryptographic key compromise response procedures MUST ensure that: a) compromised or suspected compromised cryptographic keys are immediately revoked and replaced b) replacement keys are newly generated and not derived from the compromised key c) cryptographic modules or systems are validated prior to installing replacement keys	M	U
HST04.46	The EMR Vendor MUST ensure that their keys are promptly revoked when no longer required and ensure that the key is destroyed in accordance with Requirement Category/Security Control Sections 5.0: Information Asset Management Requirements.	Cryptographic key revocation procedures MUST ensure that: a) cryptographic keys that are no longer required are promptly revoked and securely destroyed b) key revocation and destruction follow documented key management procedures c) revoked keys cannot be reused or reactivated	M	U
HST04.47	The EMR Vendor MUST ensure that the destruction of cryptographic keys is documented and auditable, with appropriate records retained to support verification and audit activities.	Cryptographic key destruction records MUST include: a) the date and time of the key material destruction b) the reason for destroying the key material c) the individual authorizing the destruction	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		d) the individual performing the destruction e) the individual(s) witnessing or validating the destruction where applicable		
HST04.48	The Chief Information Officer or their delegate MUST assign the key custodian(s) responsible for each key.	Cryptographic key management governance MUST ensure that: a) responsibility for cryptographic key management is formally assigned within the organization b) designated roles responsible for key management are documented and approved by appropriate authority c) key management responsibilities align with organizational security governance policies	M	U
HST04.49	The EMR Vendor MUST ensure that cryptographic keys and key materials are handled and protected according to their sensitivity and classification.	Cryptographic key handling controls MUST ensure that: a) cryptographic keys and related materials are handled according to organizational information classification and asset handling policies b) access to key materials is restricted based on classification and sensitivity c) handling procedures prevent unauthorized disclosure, modification, or misuse of key materials d) cryptographic key materials are stored, transmitted, and disposed of using secure handling procedures appropriate to their sensitivity	M	U
HST04.50	The EMR Vendor MUST ensure that key custodians assigned to cryptographic keys are limited to the fewest number of key custodians necessary.	Cryptographic key access management MUST ensure that: a) the number of individuals assigned to cryptographic key management roles is limited to those necessary for operational requirements b) access to cryptographic keys follows the principle of least privilege	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) key management roles and privileges are periodically reviewed		
HST04.51	The EMR Vendor MUST ensure that key custodians understand their responsibility to never disclose the key in their custody to anyone, not even to a manager or an auditor, except to another authorized key custodian for that specific key.	Cryptographic key custodian responsibilities MUST ensure that: a) individuals responsible for cryptographic keys are trained on their security responsibilities b) custodians are prohibited from disclosing key material except through authorized key management procedures c) violations of key handling policies are subject to organizational security enforcement measures	M	U
HST04.52	The EMR Vendor MUST never permit a key custodian to be the custodian for more than one key component for the same key, even if the custodianship applies to the key components at different times.	Cryptographic key separation-of-duties controls MUST ensure that: a) controls prevent a single individual from having complete control over all components or aspects of a cryptographic key where separation of duties is required b) role-based access control or equivalent mechanisms enforce separation of duties in cryptographic key management operations c) key management systems enforce authorization controls consistent with defined security policies	M	U

5.4 Vulnerability and Remediation Management

These requirements define controls for identifying vulnerabilities, assessing associated risks, and applying patches and security updates to systems and components in a timely manner.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST05.01	The EMR vendor MUST apply security updates to intrusion detection and prevention software within defined timescales (e.g. based on documented process	Security update management processes MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	or procedures) upon the discovery of a threat or vulnerability.	a) updates to intrusion detection and prevention software (e.g., signatures, rules, or engine updates) are applied in a timely manner based on defined timelines and risk levels. b) update processes are documented and consistently followed. c) updates are validated to ensure successful deployment and continued effectiveness of detection capabilities. d) update timelines are periodically reviewed to ensure alignment with evolving threat conditions.		
HST05.02	The EMR vendor and all associated or affiliated parties (employees, agents, and suppliers, including electronic service providers) MUST implement malware detection and repair software or an equivalent solution on all workstations (e.g. laptops, desktops) and servers.	Malware protection controls MUST ensure that: a) real-time protection is enabled to detect and prevent execution of malicious code b) malware definitions and detection capabilities are kept up to date through automated updates c) malware protection is deployed and enforced on all supported endpoints and servers within the environment d) malware events are logged and integrated with monitoring and incident response processes Infected systems are isolated and remediated in accordance with defined security procedures	M	U
HST05.03	The EMR Vendor MUST ensure that malware protection mechanisms and associated detection definitions are maintained at current versions across all servers, systems, and endpoints supporting the hosted EMR environment.	Malware protection update mechanisms MUST ensure that: a) malware detection signatures, threat intelligence, or protection rules are automatically updated from trusted sources b) malware protection mechanisms regularly check for updates and apply them within defined intervals c) systems verify that malware protection updates have been successfully applied across servers, systems, and endpoints	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		d) security monitoring processes notify appropriate security personnel if malware protection mechanisms fail to update or operate as expected		
HST05.04	The EMR Vendor MUST ensure that systems supporting the hosted EMR environment are regularly scanned for malware where real-time protection mechanisms are not available.	Malware detection processes MUST ensure that: a) systems not protected by real-time malware protection mechanisms are scanned for malware at defined intervals b) real-time malware protection capabilities are implemented where technically feasible to detect threats as they occur c) systems identified as infected or suspected of infection are promptly isolated from the network to prevent further propagation d) affected systems remain isolated until remediation actions have been completed and the system has been verified as free of malicious software	M	U
HST05.05	The EMR vendor or installed agent MUST scan all inbound data including physical media, email attachments, file downloads, and data transfers using malware detection software prior to data being opened or used by the system or user. Scanning MAY be carried out at different places, e.g. such as email servers, and desktop computers.	Malware scanning controls MUST include: a) Scanning of inbound data from all relevant sources, including physical media, email attachments, file downloads, and data transfers. b) Scanning performed prior to execution, access, or ingestion by the EMR Offering or user systems. c) Implementation of malware scanning at appropriate control points within the environment (e.g., email gateways, network boundaries, and endpoint devices). d) Malware scanning MAY be performed at multiple layers to provide defense-in-depth (e.g., email servers, network controls, and endpoint systems).	M	U
HST05.06	The EMR vendor MUST implement and maintain a formal vulnerability management process that includes	Vulnerability management processes MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	continuous/scheduled scanning, risk assessment of findings, and a documented remediation plan with timelines to resolution.	a) systems supporting the hosted EMR environment are regularly scanned for known vulnerabilities using automated vulnerability scanning tools or equivalent mechanisms b) identified vulnerabilities are assessed and prioritized based on risk, exploitability, and potential impact to the hosted EMR environment c) remediation activities are tracked and resolved within defined timelines based on vulnerability severity and risk level d) threat intelligence sources and vulnerability advisories are monitored to identify newly disclosed vulnerabilities that may affect the hosted EMR environment e) vulnerability prioritization considers actively exploited vulnerabilities and threat intelligence sources such as publicly maintained exploited vulnerability catalogs e.g. CISA Known Vulnerabilities Catalog (KEV).		
HST05.07	The EMR vendor or agent MUST continuously monitor information systems to identify vulnerabilities that may affect specific hardware, software, and cloud infrastructure.	Vulnerability monitoring processes MUST ensure that: a) threat intelligence sources and vulnerability advisories are monitored for newly disclosed vulnerabilities b) monitoring activities include hardware platforms, operating systems, applications, and cloud infrastructure services used by the hosted EMR environment c) newly identified vulnerabilities are assessed to determine whether affected systems require remediation or mitigation actions	M	U
HST05.08	The EMR vendor MUST ensure that vulnerability risk assessments and remediation plans are reviewed by a security analyst with independence from operational teams responsible for working in or maintaining the systems.	Review controls MUST include: a) independent validation of vulnerability severity, risk ratings, and remediation priorities.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) separation of duties to ensure that individuals responsible for remediation are not solely responsible for risk acceptance or closure decisions. c) documentation of review outcomes, including approvals, risk acceptance, or required remediation actions.		
HST05.09	The EMR vendor MUST remediate all identified vulnerabilities within a defined timeline.	The EMR vendor MUST implement a vulnerability management policy which defines timelines for remediation which MUST be reviewed, at minimum, quarterly to ensure that approved justifications are still valid.	M	U
HST05.10	The EMR vendor MUST document their timelines for reacting to a vulnerability notification. The EMR Vendor may need to provide a process/procedure document as evidence.	Vulnerability notification and triage processes MUST ensure that: a) vulnerability notifications from internal teams, external vendors, and 3rd party service providers, , security advisories, or threat intelligence sources are assessed within defined response timelines b) identified vulnerabilities are categorized or prioritized based on severity, exploitability, and potential impact to the hosted EMR environment c) triage procedures define expected timelines for assessment, mitigation, or remediation actions d) vulnerability severity classifications are used to guide remediation timelines and response priorities	M	U
HST05.11	The EMR vendor MUST implement a formal security patch management process to ensure that available patches are identified, tested and, where feasible, deployed.	The EMR vendor MUST conduct a risk-benefit analysis on all impacted systems. In cases where a decision is made not to apply a patch to one or more systems, the EMR vendor MUST also document the reason and implement compensating controls to minimize the vulnerability. Controls MAY include: a) turning off services or capabilities related to the vulnerability b) adapting or adding access controls (e.g., firewalls at the network border)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) increasing monitoring to detect or prevent actual attacks d) adapting or adding access controls (e.g., firewalls at the network border) e) increasing monitoring to detect or prevent actual attacks The risk-benefit analysis MUST have signed approval from the designated Security Officer or other authorized party.		
HST05.12	The EMR Vendor MUST assess the risks associated with applying security patches prior to deployment, including evaluating the risk posed by the vulnerability and the potential impact of applying the patch.	Patch management processes MUST ensure that: a) security patches are evaluated to determine the risk posed by the associated vulnerability and the potential operational impact of applying the patch b) patch deployment decisions consider system availability, compatibility, and potential disruption to the hosted EMR environment c) high-risk vulnerabilities are prioritized for remediation in accordance with defined vulnerability remediation timelines d) patch evaluation and deployment activities follow documented change management and testing procedures	M	U
HST05.13	The EMR Vendor MUST test and evaluate security patches prior to deployment where technically feasible to ensure they are effective and do not introduce unacceptable operational impacts.	Patch testing processes MUST ensure that: a) security patches are tested in a controlled or non-production environment prior to deployment where technically feasible b) testing activities assess the effectiveness of the patch and identify potential operational or compatibility impacts c) patch testing and deployment activities follow documented change management and system release procedures d) emergency patch deployments are documented and reviewed where pre-deployment testing is not feasible	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST05.14	The EMR Vendor MUST document and formally approve any exception to applying a security patch and manage the associated risk in accordance with the organization's vulnerability management processes.	Patch exception management processes MUST ensure that: a) decisions not to apply a patch are documented with supporting risk analysis and justification b) compensating controls or mitigation measures are implemented where feasible to reduce the risk associated with the unpatched vulnerability c) affected systems and assets are documented to ensure ongoing visibility of accepted risks d) patch exceptions are periodically reviewed to determine whether remediation or mitigation actions are required e) appropriate conforming changes to inventory records and disaster recovery plans	M	U
HST05.15	The vendor MUST review and update their information system configurations or baseline security configuration standards as appropriate, to improve their effectiveness based on the results of vulnerability scans, security advisories and evolving industry practices.	Configuration management processes MUST ensure that: a) baseline security configurations are periodically reviewed and updated based on vulnerability scan results and identified security risks b) configuration standards reflect current industry security practices and applicable security guidance c) changes to baseline configurations are documented and implemented through established change management procedures d) updated configuration standards are applied to systems supporting the hosted EMR environment	M	U
HST05.16	The EMR vendor MUST ensure that all changes to networks and information systems follow formal, documented, change control procedures.	The EMR vendor MUST include as part of the change control procedures the risk assessment and rollback plan in the event a change has a negative impact.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		All changes to networks and information systems MUST have signed approval from the designated Accountable Officer or other authorized party before any change is implemented.		

5.5 Endpoint and Perimeter Protection

These requirements define controls for protecting system endpoints and the hosting environment perimeter, including detection, prevention, and response mechanisms to mitigate unauthorized access and security threats.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST06.01	The EMR Vendor MUST disable split tunneling for remote access connections to the hosted EMR environment.	Remote access security controls MUST ensure that: a) split tunneling is disabled for VPN or remote access connections to prevent simultaneous access to external networks and the hosted EMR environment b) all remote access traffic intended for the hosted EMR environment is routed through approved security controls such as firewalls, monitoring systems, or security gateways c) remote access configurations are periodically reviewed to ensure compliance with established security policies	M	U
HST06.02	The EMR Vendor MUST require and enforce cryptographically verified identifiers for all assets connecting to the network and network zones, including data contribution endpoints and identity provider services.	Endpoint and service authentication controls MUST ensure that: a) endpoints and services connecting to protected network zones are authenticated using cryptographic mechanisms that verify system or service identity	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) authentication mechanisms may include device certificates, mutual TLS (mTLS), signed service tokens, or equivalent cryptographic identity mechanisms c) connections from endpoints or services that cannot be cryptographically authenticated are restricted or denied access to protected network zones d) identity credentials used for endpoint or service authentication are securely issued, managed, rotated, and revoked in accordance with cryptographic key management procedures		
HST06.03	The EMR vendor MUST ensure that authentication and authorization processes are in place on the hosted EMR Vendor network before access to the hosted EMR Vendor is granted.	The EMR vendor MUST ensure that no user, device, or executable process will be allowed to establish a connection without explicit verification or permission.	M	U
HST06.04	The EMR Vendor MUST isolate inbound and outbound external connections to the hosted EMR environment within a controlled network zone designed to protect internal systems.	External connection protection controls MUST ensure that: a) external network connections are terminated or inspected within a segmented network zone such as a DMZ, gateway tier, or equivalent controlled boundary b) internal systems supporting the hosted EMR environment are not directly exposed to external networks c) security controls such as firewalls, reverse proxies, or application gateways are used to control and inspect traffic entering or leaving protected network zones d) network segmentation is implemented to limit exposure of internal services and reduce the impact of potential compromises	M	U
HST06.05	The EMR Vendor MUST ensure that information system components storing data classified as internal or higher	Network segmentation controls MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	are located within protected internal network zones that are segregated from external or untrusted network zone.	a) systems storing or processing data classified as internal or higher are placed within protected network zones separated from external or less trusted network zones b) traffic between network zones is restricted and inspected according to defined security policies c) segmentation controls such as firewalls, virtual network segmentation, access control lists (ACLs), or equivalent mechanisms are used to manage and inspect traffic between zones d) access to protected network zones is limited to authorized systems and services required to support the hosted EMR environment		
HST06.06	The EMR vendor MUST install and enable firewall software on all agent and electronic service provider workstations, laptops, and where technically feasible, mobile devices that connect to and interact with the internet and hosted EMR Vendor.	Systems used to administer, support, or access the hosted EMR environment MUST be protected using host-based firewall capabilities or equivalent endpoint network protection mechanisms. These protections MUST be enabled by default and centrally managed where feasible to control inbound and outbound network traffic. Host-based firewall protections MUST be implemented on systems including but not limited to: a) vendor-managed workstations used to administer or support the EMR environment b) vendor-managed laptops used by support personnel c) servers and virtual machines within the hosted EMR environment Where technically feasible, mobile devices used by vendor personnel to access administrative functions or sensitive systems SHOULD implement equivalent network protection controls.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Firewall or endpoint protection policies MUST be periodically reviewed and maintained to ensure alignment with current security practices and operational requirements. Evidence of compliance MAY include endpoint security configuration standards, device management policies, or documentation describing host-based firewall controls implemented within the vendor environment.		
HST06.07	The EMR Vendor MUST ensure that unmanaged, insecure, or non-trusted devices, including IoT (Internet of Things) devices, are isolated from systems supporting the hosted EMR environment through network segmentation or equivalent controls.	Network segmentation controls MUST ensure that: a) IoT devices or unmanaged devices are placed in isolated network zones separate from systems supporting the hosted EMR environment b) access from these devices to protected network zones is restricted to only required services c) traffic between segmented networks is controlled and monitored using firewalls or equivalent security controls d) IoT or unmanaged devices are prevented from directly accessing sensitive systems or data unless explicitly authorized	M	N
HST06.08	The EMR vendor MUST implement mechanisms to detect and respond to malicious or unauthorized activity across systems and networks supporting the EMR Offering.	Monitoring mechanisms MUST: a) monitor systems and network activity for indicators of compromise or unauthorized behaviour b) generate alerts and security events in accordance with logging and monitoring controls c) support investigation and response to detected security events	M	U
HST06.09	The EMR Vendor MUST configure Intrusion Detection and Intrusion Prevention Systems (IDS/IPS) to generate	Intrusion detection and alerting mechanisms MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	alerts for suspicious activity, potential intrusion attempts, or violations of information security policies.	a) detection rules and alert thresholds are configured to identify suspicious or unauthorized activity b) alerts are generated for events indicating potential intrusion attempts, anomalous behavior, or violations of security policies c) detection rules and alert thresholds are periodically reviewed and updated to address evolving threats d) alerts are integrated with the organization's security monitoring and incident response processes		

6. Logging, Monitoring and Incident Management

These requirements define controls for logging, monitoring, and incident management to detect, investigate, and respond to security and privacy events, including the timely escalation and handling of incidents.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST07.01	The EMR Vendor MUST implement a centralized monitoring framework that continuously monitors, alerts, and reports on the availability, performance, and security of the hosting environment. The monitoring framework MUST provide continuous visibility across the infrastructure, platform, and application components supporting the service, regardless of whether the hosting model is physical, virtual, or cloud-based.	The centralized monitoring framework MUST include monitoring of: a) Infrastructure and facility health, including environmental and data centre conditions where applicable b) Compute and storage resources, including availability and performance of servers, storage systems, and database services c) Network services, including disruptions impacting service availability d) Backup and recovery processes, including failures and errors e) Security events, including critical alerts and intrusion detection or equivalent controls Monitoring SHALL apply to production, backup, and disaster recovery environments.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Monitoring SHOULD integrate with logging, alerting, and incident response processes to support timely detection and response to events.		
HST07.02	The EMR vendor MUST document and maintain standard operating procedures for the hosted EMR Vendor.	The operating procedures MUST specify the instructions for detailed execution of jobs including but not limited to: a) Backups and disaster recovery procedures b) System restart and startup sequences c) Error handling and alerts d) Escalation process and procedures	M	U
HST07.03	Logging MUST be enabled and operational for systems supporting the hosted EMR environment.	Logging MUST be enabled and operational for systems supporting the hosted EMR environment. Logging controls MUST ensure that: a) Logging capabilities are enabled by default on systems supporting the hosted EMR environment b) Logging services remain continuously operational c) Failures of logging mechanisms are detected and generate alerts	M	U
HST07.04	The vendor MUST ensure that all logs are classified in accordance with the highest level of information contained within the logs.	Log classification practices MUST ensure that: a) Logs are assessed and classified based on the most sensitive data elements they contain (e.g., PHI, PII, confidential system data) b) Classification levels applied to logs are consistent with organizational data classification policies and standards c) Log classification drives the application of appropriate security controls (e.g., access restrictions, encryption, retention, monitoring)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		d) Logs containing sensitive information are handled, stored, and transmitted in accordance with applicable privacy, security, and regulatory requirements e) Access to logs is restricted based on classification level and aligned with least privilege and need-to-know principles f) Classification of logs is reviewed periodically and updated where there are changes to log content, structure, or use g) Where feasible, mechanisms are implemented to minimize or mask sensitive data in logs while preserving operational and audit value		
HST07.05	The EMR Vendor MUST record security-relevant events and activities performed by users, administrators, agents, and system processes.	The EMR Vendor MUST record security-relevant events and activities performed by users, administrators, agents, and electronic service providers, including all events defined in Appendix E: Security Logging and Monitoring. Security event logging MUST ensure that: a) User activities affecting system security or data access are logged b) Administrative and operator activities are logged c) Security events identified in Appendix E are recorded	M	U
HST07.06	The vendor MUST ensure that audit logs capture sufficient information to uniquely identify the subject, object, action, timestamp, and outcome of each event.	Log content practices MUST ensure that: a) Log entries include identifiers for the subject initiating the action (e.g., user ID, system identifier, IP address) b) Log entries include identifiers for the object affected by the action (e.g., file, record, system component) c) Date and time of the event are recorded d) The event activity is captured (e.g., authentication, access, modification) e) The outcome of the event is recorded (e.g., success, failure, denied)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		f) The type of access is recorded where applicable (e.g., read, write, execute) g) Alerts or alarms generated by access control or monitoring systems are captured		
HST07.07	The vendor MUST ensure that all activities are logged in a complete and accurate manner without omission of required audit data.	Log collection practices MUST ensure that: a) Log data is captured in its original form at the source system b) Filtering, aggregation, or transformation does not result in the loss of relevant security or operational information c) Where log reduction is required, it is performed downstream in a controlled and auditable manner d) Log collection configurations are documented and maintained	M	U
HST07.08	The EMR Vendor MUST ensure that logs are generated from trusted sources and include accurate timestamps.	The EMR Vendor MUST ensure that logs are generated from trusted sources and include accurate and reliable timestamps. Log source controls MUST ensure that: a) System clocks are synchronized to a trusted time source b) Changes to log sources are controlled, logged, and managed through documented change management procedures	M	U
HST07.09	The EMR Vendor MUST protect the confidentiality, integrity, and availability of logs.	The EMR Vendor MUST protect the confidentiality, integrity, and availability of logs. Log protection controls MUST ensure that: a) Access to logs is restricted based on least privilege and need-to-know b) Logs are protected against unauthorized modification or deletion c) Logs are protected during storage and transmission	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		d) Individuals with access to logs cannot modify, delete, or disable logs of their own activities		
HST07.10	The vendor MUST maintain a list of all agents or electronic service providers who have authorized access to logs.	At a minimum, the list MUST contain: a) Full name of the agent or electronic service provider b) Work phone number of the agent or electronic service provider c) Work email address of the agent or electronic service provider d) ID that the agent or electronic service provider uses to logically access the log	M	U
HST07.11	The vendor MUST not configure logs to overwrite old data when the maximum log size limit has been reached.	Log retention and storage practices MUST ensure that: a) Log storage capacity is proactively monitored and managed to prevent loss of log data due to capacity constraints b) Automated controls and alerting mechanisms are in place to notify administrators when log storage thresholds are approaching capacity limits c) Log retention policies are defined and enforced to ensure logs are retained for required periods in accordance with legal, regulatory, and organizational requirements e.g. Client data retention policies, Treasury Board Policy on Service and Digital. d) Mechanisms are implemented to prevent deletion or modification of logs outside of defined retention and disposition processes (e.g., immutability controls, write-once storage) e) When storage limits are reached, logs are archived, rotated, or offloaded to secondary storage in a manner that preserves integrity, availability, and auditability f) Log retention and archival processes ensure that historical logs remain accessible for audit, investigation, and compliance purposes	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		g) Any log disposal processes are controlled, auditable, and performed in accordance with approved retention schedules and data handling policies		
HST07.12	The vendor MUST ensure that the management of log generation sources is logged and controlled via documented change control procedures.	Log source management controls MUST ensure that: a) Changes to logging configurations or sources are formally documented, approved, and implemented through established change control procedures b) Changes are recorded, including the nature of the change, the individual performing the change, and the timestamp c) Logging configurations are protected from unauthorized modification d) Access to modify logging configurations is restricted to authorized personnel based on least privilege e) Changes to logging configurations are auditable and subject to review f) Unauthorized changes to logging configurations are detected and generate alerts	M	U
HST07.13	The EMR Vendor MUST implement centralized log collection and processing capabilities.	The EMR Vendor MUST implement centralized log collection and processing capabilities. Centralized logging controls MUST ensure that: a) Logs from multiple systems are aggregated to centralized log management systems b) Logs are normalized or standardized to support analysis and correlation	M	U
HST07.14	The EMR Vendor MUST monitor logs using automated mechanisms to detect suspicious activity or potential security incidents.	The EMR Vendor MUST monitor logs using automated mechanisms to detect suspicious activity or potential security incidents. Log monitoring controls MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		a) Automated analysis tools monitor logs for anomalous activity b) Correlation mechanisms identify patterns across multiple systems c) Automated alerts are generated for security-relevant events		
HST07.15	The vendor MUST review logs to detect anomalous events, policy deviations, or potential security incidents affecting the network or the hosted EMR environment.	Log review practices MUST ensure that: a) Logs are reviewed on a defined regular schedule to identify anomalous activity or behaviour outside of established policies and procedures b) Automated alerts and flagged events are included in log reviews to support detection of potential attacks or unauthorized activities c) Log reviews consider activity from users, administrators, agents, and electronic service providers d) Findings from log reviews are documented and escalated for further investigation where required	M	U
HST07.16	The vendor MUST ensure that information system administrator and operator logs are reviewed.	Log review practices MUST ensure that: a) Logs of administrators and operators are reviewed at a defined regular period to identify anomalous or unauthorized activities b) Reviews focus on privileged activities that may impact system security, configuration, or access to sensitive data c) Results of log reviews are documented and retained for audit and compliance purposes	M	U
HST07.17	The vendor MUST ensure that segregation of duties MUST exist for all log reviews, e.g., someone other than the information system administrator MUST review the logs for the information system they manage.	Segregation of duties for log review MUST ensure that: a) Log reviews are performed by individuals independent of the activities or systems being reviewed b) Individuals with administrative or privileged access do not review their own activities	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) Responsibilities for log generation, management, and review are appropriately separated to prevent conflicts of interest d) Exceptions to segregation of duties (if unavoidable) are documented, justified, and subject to compensating controls		
HST07.18	The vendor MUST ensure that their logs relating to production data are readily available online, at a minimum, for six months.	Log availability practices MUST ensure that: a) Production logs are accessible online to support timely monitoring, investigation, and audit activities b) Online access supports efficient search, retrieval, and analysis of log data	M	U
HST07.19	The vendor MUST ensure that logs related to backups are readily available online for the same period as logs related to production data.	Backup log practices MUST ensure that: a) Backup-related logs are subject to the same availability requirements as production logs b) Backup logs are accessible for monitoring, validation, and audit purposes	M	U
HST07.20	The vendor MUST retain archived information system logs, including logs of HIC, agent, and electronic service provider activities, in accordance with regional or jurisdictional data retention policies. E.g. The Electronic Health Record Retention Policy and Procedure Ontario Health.	Log retention practices MUST ensure that: a) Retention periods are defined and enforced in accordance with applicable policies and regulatory requirements b) Archived logs remain accessible and usable for audit, investigation, and compliance purposes c) Retention applies consistently across all relevant user types, including HICs, agents, and service providers	M	U
HST07.21	The EMR Vendor MUST manage the archival, storage, retrieval, and disposal of logs in accordance with defined data retention and information asset management policies.	Log archival and lifecycle management processes MUST ensure that: a) archived logs are stored in formats that support restoration and review throughout the retention period	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) archived logs are labeled, indexed, or otherwise organized to enable efficient retrieval for audit, investigation, or compliance purposes c) archived logs are protected against unauthorized access, modification, or loss during the retention period d) logs are securely disposed of in accordance with information asset management and data retention policies once the retention period expires		
HST07.22	The EMR vendor MUST maintain and consult their documented information security and incident handling process immediately upon the detection or prevention of a security incident by their IDS/IPS.	The EMR vendor MUST develop and maintain an incident “playbook” for the handling of different types of IDS/IPS events to ensure that approved documented procedure and handling is followed. Examples MAY include DDOS, Ransomware, Brute-force, etc.	M	P

7. Business Continuity and Disaster Recovery

These requirements define controls to ensure the continuity and recovery of EMR services, including the ability to meet defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) during service disruptions and disasters.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST08.01	The EMR vendor MUST ensure that they implement and maintain a Business Continuity and Disaster Recovery (BCDR) strategy that accounts for Information Security and Information Technology within the core solution.	The EMR vendor MUST ensure that the BCDR solution maintains the availability of clinical data and the rapid recovery of all services following a disruption inclusive of the following: a) Developing a resilient technical infrastructure including disaster recovery plans b) Coordinating and maintaining business continuity plans and arrangements c) Validating business continuity plans to ensure requirements can be met Inclusion of a RACI (Responsible, Accountable, Consulted, Informed) chart for BCDR activities.	M	U
HST08.02	The EMR vendor MUST maintain a business continuity strategy that includes a comprehensive inventory of all information systems that are supported by the BCDR plan.	The EMR vendor MUST formalize the inventory within a Business Continuity Risk Register that explicitly ranks systems by criticality and identifies all essential internal and external stakeholders required for service restoration.	M	U
HST08.03	The EMR Vendor MUST implement a notification and alerting service to communicate timely and reliable information to subscribers and EMR users regarding service disruptions, outages, and disaster events that may impact the availability or delivery of the EMR Offering and related services.	The notification and alerting service MUST issue alerts for: a) Planned and unplanned service outages b) Outages or errors affecting interfaces to Provincial EHR Solutions and Services c) Outages or errors affecting other integrated interfaces d) Any overall service disruption impacting the EMR Offering e) Disaster events or conditions that may affect the delivery of the EMR Offering or related services	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		The notification and alerting service MUST ensure that: i. Subscribers and EMR users receive timely, accurate, and actionable information regarding service disruptions ii. Notifications support continuity of operations during service disruptions and disaster events iii. Communication is maintained throughout the duration of the disruption, including status updates where applicable The vendor MUST be capable of delivering alerts and notifications through multiple communication channels, including but not limited to: I. Email II. Telephone III. Web-based notifications IV. Mobile device messaging V. Fax		
HST08.04	The EMR vendor MUST develop and maintain a Business Continuity Plan (BCP) for each critical information system or group of related information systems as part of the overarching BCP strategy.	An EMR Offering is foundational to the operation of a subscriber's and user's medical practice. If an EMR Offering is unavailable, affected subscribers and users MUST be able to continue the operation of their medical practices during unplanned outages. The vendor's business continuity plan MUST contain at a minimum: a) The criteria to be used by the vendor in deciding when business continuity processes should be invoked and terminated b) How subscribers will be notified of the outage, the remedies, expected duration and its ongoing status c) Recommended interim processes to be followed by subscribers once an outage has been declared d) Any vendor support services that will be available during the outage such as: I. Offline and read-only access to patient files	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		II. Access to daily schedules by users III. Recording of patient encounters by users Updating and synchronizing records as applicable once the operation of an EMR Offering has been restored.		
HST08.05	The EMR vendor MUST formally designate an owner for each information system or group of related information systems.	The EMR vendor MUST ensure that the owner is personally accountable and professionally competent for developing, testing, and executing BCP and making recovery arrangements.	M	U
HST08.06	The EMR vendor MUST derive all business continuity plans from the formal, documented, risk assessment.	The EMR vendor MUST ensure that this formalized process includes the following: a) Assessing the potential business impacts associated with the disruption of critical information systems b) Evaluating the likelihood of critical information systems being disrupted based on a set of scenarios of possible disasters or disruptions Obtaining sign-off from a senior-level executive (e.g., the CIO) for selective suitable business continuity plans and arrangements to treat the risks identified	M	U
HST08.07	The EMR vendor MUST create a Business Continuity Plan (BCP) for all critical information systems.	The EMR vendor MUST ensure that the BCP details the following: a) Conditions for their invocation b) Arrangements for the secure storage of plans (e.g., offsite) and their retrieval in case of emergency c) The maximum tolerable period of disruption, i.e., the maximum period of time that the organization can withstand a disruption of information system(s) d) A schedule of recovery tasks and activities to be carried out including, emergency fallback and resumption procedures (in priority order)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		e) The roles and responsibilities for carrying out each task and activity f) Information security controls to be applied following invocation of the business continuity plan (e.g., to protect the confidentiality and integrity of the information) g) Tasks to be undertaken following a recovery and restoration (e.g., checking that systems and information are restored to the same state they were in before the business continuity plan was invoked)		
HST08.08	The EMR vendor MUST conduct a formal review and technical test of their Business Continuity Plan (BCP) annually.	The EMR vendor MUST ensure that testing for the following scenarios is completed annually: a) Simple tests, which involve structured walk-through tests where stakeholders meet to rehearse the business continuity plan using different scenarios b) Medium tests, which involve simulation tests where staff test the business continuity plan using specific scenarios and parallel tests where alternative facilities are used to avoid disrupting production information systems c) Complex tests, which involve failover and full-interruption tests where the original site is shut down, and a complete test is performed at an alternative facility	M	P
HST08.09	The EMR vendor MUST maintain a formal, documented, record for every Business Continuity Plan (BCP) test that is executed.	The EMR vendor MUST ensure that documentation used to track BCP tests include the following: a) Date of the documented test b) Scope of testing and/or test objectives c) Detailed analysis of the result	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Sign-off from a senior-level executive (E.g. CIO).		
HST08.10	The EMR Vendor MUST support a Point-in-Time Recovery (PITR) capability that enables the restoration of data and system state in time following a failure. The PITR capability MUST support restoration within defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO) targets.	The EMR Vendor MUST implement a PITR solution that: a) Support automated snapshots of the system b) Allow restoration of data or the environment to a specific date or time in the event of a system failure c) Ensure that the supported Recovery Point Objective (RPO) is defined and documented d) Be capable of minimizing data loss and operational impact on subscribers and EMR users	M	U
HST08.11	The EMR vendor MUST implement an automated backup system for the hosted EMR Offering that creates a complete, restorable copy of all EMR data inclusive of PHI and logs.	The backup system SHALL: a) Capture all EMR data repositories, including databases, file storage, attachments, and system logs necessary to support operational and forensic recovery b) Create consistent backup sets that support restoration to a defined point in time c) Operate automatically according to a documented backup schedule d) Protect backup data in transit and at rest in accordance with cryptographic requirements e) Be monitored for backup failures and generate alerts in accordance with logging and monitoring requirements f) Support restoration testing on a periodic basis Where the EMR Offering is deployed in a vendor-hosted or cloud environment, backups SHALL include sufficient system configuration and application state information to restore the hosted environment to an operational state.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Where the EMR Offering is deployed in a local (on-premise) environment, backups SHALL include sufficient system configuration, application components, and data to restore the EMR system to an operational state on replacement or rebuilt infrastructure.		
HST08.12	The EMR vendor MUST ensure that their backup and disaster recovery plan is documented and includes data recovery objectives.	Backup and disaster recovery planning processes MUST ensure that: a) recovery time objectives (RTO) and recovery point objectives (RPO) are defined for systems and data supporting the hosted EMR environment b) recovery objectives align with business and operational requirements for system availability and data protection c) the disaster recovery plan is formally approved by appropriate management or designated security authorities d) the plan is periodically reviewed and updated to reflect changes in systems, infrastructure, or operational requirements	M	U
HST08.13	The EMR vendor MUST ensure that all backups are stored in a remote location, at a sufficient geographical distance from the primary data centre location to escape any damage due to disaster.	Backup storage SHALL: a) Be located in a geographically distinct region from the primary production environment b) Be selected to reduce the risk of simultaneous impact from natural, environmental, or infrastructure-related events c) Align with defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements d) Maintain the same security controls and protections applied to primary data Where cloud services are utilized, backups MAY be stored in a separate availability zone or region, provided the separation supports recovery objectives and resilience requirements.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Where on-premise deployments are used, backups SHALL be stored off-site in a geographically distinct location.		
HST08.14	The EMR vendor MUST encrypt and secure all backups containing PHI both at rest (stored) and in transit (between sites or moved).	Backup protection controls MUST ensure that: a) backups containing sensitive or regulated data are encrypted while stored and during transmission between systems or sites b) encryption mechanisms used for backups comply with approved cryptographic standards and key management practices c) access to encrypted backups is restricted to authorized personnel or systems responsible for backup and recovery operations d) cryptographic keys used to protect backups are managed in accordance with the organization's cryptographic key management processes	M	U
HST08.15	The EMR vendor MUST ensure that any environment storing, processing, or providing access to EMR data — including backup repositories, replicated environments, and reporting or data warehouse systems — is protected by security controls equivalent to those applied to the primary hosted EMR environment.	The EMR vendor MUST ensure that equivalent protection includes, as applicable: a) Access control and authentication mechanisms consistent with the primary hosted environment b) Network segmentation and boundary protection controls c) Encryption standards for data at rest and in transit d) Logging and monitoring capabilities consistent with production systems e) Physical and environmental safeguards appropriate to the hosting model The EMR vendor MUST ensure that this equivalency is maintained regardless of whether the infrastructure is vendor-managed, cloud-based, or hybrid.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST08.16	The EMR vendor MUST perform regular backup and recovery tests on all media (physical or virtual) at defined intervals, at minimum, annually.	The EMR vendor MUST log all backup failures as part of their incident management process and document the steps taken to remediate and retest the backup.	M	U
HST08.17	The EMR vendor MUST regularly test their restoration procedures to ensure they are effective and can be completed within their Recovery Time Objective (RTO) as defined within their operational procedures for recovery.	At a minimum, a full restoration test MUST be conducted and documented annually.	M	U
HST08.18	The EMR vendor MUST provide a robust and reliable hosting environment for the EMR Offering.	The EMR vendor MUST ensure that the hosted EMR Offering is highly available and supported by alternate or duplicate (failover) facilities that can assume full production workloads in the event of a primary site failure, and that mechanisms are in place to identify, recover, and reconcile transactions following a system failure.	M	U
HST08.19	The EMR vendor MUST implement and proactively address risk of critical system malfunctions.	The EMR vendor MUST ensure that the following methods of risk reduction include: a) Procurement of modern, standardized, and actively supported hardware and/or software b) Ensuring compliance with common or industry security standards for hardware and software c) Giving high priority to reliability, compatibility and capacity during the acquisition process d) Utilization of a resilient telecommunications infrastructure to ensure stable service delivery	M	U
HST08.20	The EMR vendor MUST architect a highly resilient network infrastructure which will minimize single points of failure.	The EMR vendor MUST ensure that the network is capable of the following: a) Automatic network traffic rerouting when critical network equipment or links fail	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		b) Installing duplicate or alternative network components (e.g., assets, hubs, bridges, concentrators, switches, firewalls and network traffic filters) to critical communications equipment, or c) Arranging fallback to alternative points of connecting and links with external service providers		
HST08.21	The EMR vendor MUST establish a fault management framework to identify, document and resolve system failures.	The EMR vendor MUST ensure that the fault management framework includes the following: a) Recording all actual or suspected faults b) Notifying affected parties of faults in a timely manner c) Disabling information systems and services with suspected faults until adequately remedied d) Ensuring that critical information systems are repaired or replaced within critical timescales	M	R
HST08.22	The EMR vendor MUST configure data archiving of the hosted EMR Vendor as determined by the record retention requirements of the information they contain and in accordance with any legal or regulatory requirements.	The EMR vendor MUST be aware of the following data archiving guidelines. d) Adults – 10 years from the date of the last entry e) Minors (<18) - 10 years after the patient turns (or would have turned) 18 f) Deceased - 10 years from the date of the last entry g) Billing - 7 years	M	U

8. Acceptable Use of Information and Information Technology

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST09.01	The EMR vendor MUST ensure that every person, including staff, contractors, and third-party suppliers, including any automated services, uses a unique individual identifier and secure password/credential to access the EMR remotely.	The EMR vendor MUST require the use of an assigned ID and password for remote access hosted EMR environments. This MUST include any session where the EMR Vendor, staff, agents, or suppliers access the EMR, its supporting systems for troubleshooting, maintenance, or general client support.	M	U
HST09.02	The EMR vendor MUST ensure that all personnel, including staff, contractors, and third-party suppliers are informed that they MUST maintain exclusive control over their assigned ID and password to access the EMR Vendor remotely.	The EMR vendor MUST maintain effective policies and/or procedures for remove access which includes the following: a) Information outlining the intended use of their assigned ID and password b) Statement indicating that shared access is prohibited The EMR vendor SHOULD implement appropriate logging to ensure that actions performed remotely by any staff, contractor, or third-party supplier is non-reputable.	M	U
HST09.03	The EMR vendor MUST restrict access for all persons who access the hosted EMR Vendor to the minimum extent necessary to perform their specific (authorized) duties.	The EMR vendor MUST ensure that access is granted in accordance with The EMR Vendor's own privacy policies based on the principal of least privilege and need-to-know (e.g., providing or assisting in the provision of health care, or it is expressly authorized by the HIC in cases of providing support).	M	U
HST09.04	All Persons, employees or Vendor agents, MUST immediately report suspected or confirmed information security incidents to the designated EMR support point of contact (e.g., a	Examples of information security incidents include, but are not limited to: a) Unauthorized disclosure of PHI b) Theft or loss of information technology that contains PHI even if it is encrypted c) Virus or malware infection on a device that has access to the hosted EMR Vendor	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	help desk or system administrator). Alternatively, Persons may report the incident to their manager or supervisor, who in turn MUST report it to the applicable incident response contact.	d) Attempts (either failed or successful) to gain unauthorized access to the hosted EMR Vendor e) Compromised password, i.e., another individual knows your password		
HST09.05	All Persons, employees or Vendor agents, MUST provide their full cooperation to the vendor, their agents or electronic service providers with any information security incident investigation.	Investigation support practices MUST ensure that: a) Persons understand their obligation to cooperate with investigations b) Information requested during investigations is provided in a timely manner c) Cooperation requirements are communicated through policy and training d) Non-cooperation is addressed through enforcement procedures	M	U
HST09.06	All Persons, employees or Vendor agents, MUST never attempt to exploit any suspected security weakness, even to explore that such weakness may exist, unless it is part of their assigned job duties or responsibilities and they are explicitly authorized by the vendor to do so.	Acceptable use practices MUST ensure that: a) Security testing or probing activities are only performed by authorized individuals b) Unauthorized attempts to identify vulnerabilities are prohibited c) Authorized testing activities are formally approved and documented d) Violations are subject to disciplinary processes	M	U
HST09.07	All Persons, employees or Vendor agents, MUST never knowingly perform an act that will interfere with the normal operation of the hosted EMR Vendor instance, or try to disrupt the system by either intentionally making services unavailable or by affecting the	System protection practices MUST ensure that: a) Activities that could disrupt system availability or integrity are prohibited b) Users are aware of actions that may unintentionally impact system operations c) Monitoring mechanisms exist to detect disruptive behaviour d) Violations are investigated and addressed	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	integrity of the data being stored in or processed by the EMR.			
HST09.08	All Persons, employees or Vendor agents, MUST abide by the terms and conditions provided by the EMR vendor.	Acceptable use governance MUST ensure that: a) Terms and conditions are communicated and accessible to all users b) Users acknowledge and accept acceptable use requirements c) Compliance with terms is monitored and enforced d) Terms are periodically reviewed and updated	M	U
HST09.09	All Persons, employees or Vendor agents, MUST never discuss PHI with any person who does not have a need-to-know or is not authorized to know the information.	Information handling practices MUST ensure that: a) PHI is only shared with authorized individuals with a valid need-to-know b) Access decisions are based on defined roles and responsibilities c) Unauthorized disclosure risks are communicated through training d) Violations are subject to investigation and corrective action	M	U
HST09.10	All Persons, employees or Vendor agents, MUST never discuss PHI in public areas, including elevators, as it may be easily overheard by those who do not have a need-to-know.	Privacy protection practices MUST ensure that: a) PHI is not discussed in environments where it may be overheard b) Users are aware of risks associated with public or shared spaces c) Privacy awareness training reinforces appropriate communication practices d) Sensitive discussions are conducted in secure environments	M	U
HST09.11	All Persons, employees or Vendor agents, MUST lock up PHI in any form (e.g., locking paper, printed copies originating from the hosted EMR Vendor, EMR offering, or portable storage media in a cabinet) when left unattended in an	Physical security practices MUST ensure that: a) PHI in physical form is secured when unattended b) Storage mechanisms (e.g., locked cabinets) are used appropriately c) Access to physical records is restricted to authorized individuals d) Physical security controls are consistently applied	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	unsecured area, especially when the office or area is vacated.			
HST09.12	All Persons, employees or Vendor agents, MUST always log off or lock unattended computers or workstations to prevent unauthorized individuals from accessing PHI.	Workstation security practices MUST ensure that: a) Systems are locked or logged off when unattended b) Session timeout or auto-lock controls are implemented where possible c) Users are trained on securing active sessions d) Unauthorized access risks are minimized	M	U
HST09.13	All Persons, employees or Vendor agents, MUST only store PHI on approved devices or storage networks and only store the minimal amount necessary to fulfill the specific task or business requirement.	Data storage practices MUST ensure that: a) PHI is stored only on approved devices or systems b) The amount of PHI stored on portable media is minimized c) Portable media is encrypted and controlled d) Storage practices align with organizational policies	M	U
HST09.14	All Persons, employees or Vendor agents, MUST always ensure that paper documents containing PHI are shredded or placed in a secure shredding receptacle when they are no longer needed.	Media disposal practices MUST ensure that: a) Paper records containing PHI are securely destroyed b) Approved shredding or disposal methods are used c) Disposal processes prevent reconstruction of PHI d) Disposal practices are consistently followed	M	U
HST09.15	All Persons, employees or Vendor agents, MUST follow internal procedures for the proper secure disposal of any information technology that may have PHI stored on it.	Device disposal practices MUST ensure that: a) Devices containing PHI are sanitized prior to disposal b) Approved disposal or destruction procedures are followed c) Data cannot be recovered after disposal d) Disposal activities are documented where required	M	U
HST09.16	All Persons, employees or Vendor agents, MUST only communicate	Email usage practices MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	(e.g. email) PHI when it is necessary for providing or assisting in the provision of health care or in support of associated business operations. The communication of PHI MUST comply with established organizational policies and procedures for the EMR Offering.	a) PHI is transmitted only when necessary and permitted b) Email usage aligns with organizational policies c) Risks of transmitting PHI via email are understood d) Alternative secure methods are used where appropriate		
HST09.17	All Persons, employees or Vendor agents, MUST encrypt all communication (e.g. email) that contains PHI using a secure file transfer solution or a secure messaging system that meets established security standards for the EMR Offering.	Secure transmission practices MUST ensure that: a) PHI transmitted electronically is protected using approved encryption methods b) Secure email or file transfer solutions are used c) Encryption methods comply with organizational standards d) Transmission risks are minimized	M	U
HST09.18	All Persons, employees or Vendor agents, MUST never use external email accounts (e.g., Hotmail, or Gmail) to send or receive PHI.	Email control practices MUST ensure that: a) External or personal email accounts are not used for PHI b) Approved communication channels are enforced c) Monitoring controls detect unauthorized usage d) Violations are addressed	M	U
HST09.19	All Persons, employees or Vendor agents, MUST create passwords that meet the minimum length and complexity requirements defined in Appendix B: Minimum Password Requirements.	Password complexity practices MUST ensure that: a) passwords meet minimum length thresholds b) passwords include required character types c) complexity rules align with organizational standards d) password strength reduces susceptibility to guessing or brute force attacks	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST09.20	All Persons, employees or Vendor agents, MUST ensure that passwords are not easily guessable and do not contain predictable or personally identifiable information.	Password usage practices MUST ensure that: a) users maintain exclusive control of their credentials b) shared or generic password use is prohibited c) password reuse across systems is minimized d) compromised credentials do not impact multiple systems	M	U
HST09.21	All Persons, employees or Vendor agents, MUST choose passwords that are easy to remember but hard to guess by someone else.	Password initialization practices MUST ensure that: a) temporary passwords are not used beyond first login b) users are prompted to change passwords upon first authentication c) reset processes enforce password change before access is granted d) initial credentials are not reused	M	U
HST09.22	All Persons, employees or Vendor agents, MUST never change passwords in an easily recognized pattern (e.g., changing "lL0v3EatingP!zza1" to "lL0v3EatingP!zza2").	Password protection practices MUST ensure that: a) passwords are not stored in plain text b) physical recording of passwords is minimized or controlled c) users are trained on secure handling of credentials d) unauthorized access to stored credentials is prevented	M	U
HST09.23	All Persons, employees or Vendor agents, MUST ensure that their passwords used to access the EMR system are different from their password(s) used to access other accounts (e.g., corporate e-mail account, personal banking, etc.).	Credential management practices MUST ensure that: a) credentials are not hard coded in scripts or configuration files b) secure credential storage mechanisms are used c) access to stored credentials is restricted d) automated processes use secure authentication methods	M	U
HST09.24	All Persons, employees or Vendor agents, MUST ensure that passwords	Password transmission practices MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	are protected during authentication and are not exposed through insecure transmission or handling practices.	a) passwords are protected using encrypted transmission channels b) insecure transmission methods are not used c) authentication exchanges are protected from interception d) transmission mechanisms comply with organizational security standards		
HST09.25	All Persons, employees or Vendor agents, MUST keep their passwords a secret, never telling anyone their password, including a system administrator, help desk personnel or a manager.	Password storage practices MUST ensure that: a) passwords are hashed using approved algorithms b) salting or equivalent protections are applied c) password storage mechanisms prevent retrieval of original values d) storage practices align with cryptographic standards	M	U
HST09.26	All Persons, employees or Vendor agents, MUST change their password immediately if they suspect or confirm that their password has been disclosed or compromised.	Authentication control practices MUST ensure that: a) repeated failed authentication attempts trigger account logout b) logout thresholds are defined and enforced c) logout duration deters brute force attacks d) monitoring exists for repeated authentication failures	M	U
HST09.27	All Persons, employees or Vendor agents, MUST not include their ID or password in any automated sign-on process (e.g., stored in a macro or function key).	Credential compromise practices MUST ensure that: a) compromised credentials are immediately invalidated b) users are notified of suspected compromise where appropriate c) password reset processes are enforced promptly d) monitoring supports detection of credential compromise	M	U
HST09.28	All Persons, employees or Vendor agents, MUST always change passwords that are provided to them at initial login.	Password history practices MUST ensure that: a) password history controls are enforced b) users cannot reuse previously used passwords within defined limits c) password reuse restrictions align with organizational policy d) controls reduce risk of repeated credential compromise	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST09.29	All Persons, employees or Vendor agents, MUST use an approved remote access solution (e.g., through a virtual private network or terminal services) to remotely access the EMR Offering or connected service	Remote access practices MUST ensure that: a) Only approved remote access solutions are used b) Remote connections are secured and authenticated c) Access is restricted to authorized users d) Remote access risks are minimized	M	U
HST09.30	All Persons, employees or Vendor agents, MUST follow the proper procedures to disconnect from remote access (e.g., if the remote access solution has a disconnect option, use this option to disconnect rather than simply closing the application).	Remote session management practices MUST ensure that: a) Sessions are properly terminated using approved methods b) Improper disconnection does not leave sessions exposed c) Users are trained on proper disconnection procedures d) Session risks are minimized	M	U
HST09.31	All Persons, employees or Vendor agents, MUST never access the EMR Offering or connected service in an area where unauthorized individuals can view the information (e.g., Internet cafés, public transit, and other non-private settings).	Privacy protection practices MUST ensure that: a) PHI is not accessed in environments where it can be observed by unauthorized individuals b) Users assess environmental risks before accessing systems c) Public access scenarios are restricted d) Visual privacy risks are minimized	M	U
HST09.32	All Persons, employees or Vendor agents, MUST never leave their mobile computing device that has the ability to access the EMR Offering or connected service unattended in a public place.	Mobile device security practices MUST ensure that: a) Devices are not left unattended in public areas b) Physical control of devices is maintained at all times c) Theft or loss risks are minimized d) Users are trained on mobile device security	M	U
HST09.33	All Persons, employees or Vendor agents, MUST, when required to	Mobile device protection practices MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	leave their mobile computing device in a vehicle, lock it in the trunk or place it out of view before getting to their destination. If they get to the destination before securing the device, they should take it with them instead.	a) Devices left in vehicles are concealed and secured b) Physical exposure risks are minimized c) Alternative secure handling is used where possible d) Users are aware of theft risks and mitigation measures		

9. Information and Asset Management

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST10.01	The EMR vendor MUST implement a formal classification scheme that categorizes all information and assets, both physical and digital, based on their Confidentiality, Integrity, and Availability (CIA).	Refer to Appendix F: Information Asset Management within this document for more information.	M	P
HST10.02	The EMR vendor MUST label all information and assets in accordance with their internal classification scheme.	The EMR vendor MUST ensure that labels are applied to physical hardware (E.g. laptops, servers, backup drives) and digital assets (databases, files to clearly indicate their sensitivity and importance/criticality. Refer to Appendix F: Information Asset Management within this document for more information.	M	P
HST10.03	The EMR vendor MUST ensure that all PHI and all assets, inclusive of hardware, software, and staff, that process or store PHI are	The EMR vendor MUST ensure that this protection is active and maintained throughout the lifecycle of the data, from collection to eventual destruction. Refer to Appendix F: Information Asset Management within this document for more information.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	protected in accordance with PHIPA.			
HST10.04	The EMR vendor MUST ensure that information of different classification levels have applied to them the highest classification level for the entire dataset.	The EMR vendor MUST handle, store, and protect all data according to the most secure controls required by any single piece of information within it.	M	P
HST10.05	The EMR vendor MUST assign a unique identifier to every printed or physical copy of material that is classified as restricted at the time of its creation.	The EMR vendor MUST maintain a master list that records the unique identifier of paper material and the identity of the individual, staff or agent, to whom it was distributed to or claimed by.	M	P
HST10.06	The EMR vendor MUST record/log the destruction of PHI as soon as possible, and no later than five business days after its destruction.	The EMR vendor MUST ensure that the record/log contains at a minimum the following detail: a) Date that the PHI was destroyed b) Description of the scope of PHI that was destroyed c) Description of how the PHI was destroyed (E.g. Cryptographic erasure or NIST compliant shred) d) Identity of the person who destroyed the PHI e) Identity of the person who authorized the destruction of PHI f) Identity of the person who verified the completeness of the destruction	M	P

10. Physical Security

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST11.01	The EMR Vendor MUST ensure that physical and environmental security	Physical security practices MUST ensure that:	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	controls are implemented to protect systems supporting the hosted EMR environment from unauthorized access and environmental risks.	a) Physical access to facilities and systems is restricted to authorized individuals b) Controls are implemented to protect against environmental threats (e.g., fire, flooding, power disruption) c) The level of physical security is commensurate with the sensitivity of the information (including PHI) and system criticality d) Controls apply to both vendor-managed and third-party hosted environments, as applicable		
HST11.02	The vendor MUST ensure that the strength of each perimeter depends on the physical security requirements of the information and information technology within the perimeter and, if applicable, the results of a threat risk assessment (TRA).	Physical security design practices MUST ensure that: a) Physical security controls are proportionate to identified risks and business impact b) Threat and risk assessments consider facility exposure, location risks, and data sensitivity c) Results of the TRA are used to define and adjust physical security controls	M	U
HST11.03	The EMR vendor MUST ensure that any facility, both managed or cloud-hosted, are protected against unauthorized physical access to any system that stores or processes PHI or any restricted information.	The EMR vendor MUST ensure that regardless of the hosted model chosen that physical access for the prevention of intrusion has been implemented. Examples MAY include: a) Fitting vulnerable doors and windows with locks or bolts b) Installing and monitoring closed-circuit television (CCTV) c) Employing security guards d) Installing intruder detection systems on external doors and testing accessible windows regularly.	M	R
HST11.04	The EMR vendor MUST ensure that highly sensitive facilities are located away from areas that are easily accessible to the public.	The EMR vendor MUST treat details about highly sensitive facilities confidential. E.g. by using discrete signs or excluding details from directories or telephone books.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST11.05	The vendor MUST clearly define and document the information security responsibilities of all their agents, staff, and electronic service providers with access to the hosted EMR Offering.	Information security responsibility practices MUST ensure that: a) roles and responsibilities are clearly defined for employees, agents, and electronic service providers b) responsibilities align with access privileges and job functions c) responsibilities are documented and communicated to all applicable personnel d) accountability for security-related activities is established and maintained	M	U
HST11.06	The vendor MUST implement personnel screening and verification processes for individuals who will have access to the hosted EMR Offering.	Personnel verification practices MUST ensure that: a) character or employment references are obtained where appropriate b) criminal record checks are conducted where applicable and permitted c) prior experience, education, and professional qualifications are verified d) identity is validated using government-issued identification e) screening practices are proportionate to the level of access and associated risk	M	U
HST11.07	The vendor MUST ensure that personnel with access to the hosted EMR Offering formally acknowledge and agree to their information security responsibilities.	Personnel agreement practices MUST ensure that: a) individuals agree to adhere to the vendor's information security policies b) legal responsibilities and rights related to information protection and privacy are communicated c) confidentiality or non-disclosure obligations are established and extend beyond the term of engagement d) information security responsibilities apply during and outside normal working conditions, including after termination of access	M	U
HST11.08	The vendor MUST ensure that visitor access to highly sensitive facilities is controlled and managed.	Visitor access controls MUST ensure that: a) Permitted physical access only for specific, authorized purposes a) Monitored by recording arrival and departure times b) Obligated to wear visitor badges at all times c) Supervised at all times d) Made aware of behaviour or actions that are prohibited (e.g., filming or photography)	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST11.09	Restricted information is protected from power failures and other disruptions caused by failures in supporting utilities (e.g., electricity, water supply, heating/ventilation, and air conditioning), including where such controls are implemented by third-party hosting or cloud service providers.	Utility protection practices MUST ensure that: a) systems supporting restricted information are protected against disruptions from utility failures (e.g., power, water, HVAC) b) controls are implemented to maintain availability during utility disruptions c) supporting utilities are monitored and maintained to prevent service interruptions d) contingency measures are in place to support continuity of operations during failures	M	U
HST11.10	The vendor MUST ensure that power cabling supporting highly sensitive facilities is protected from damage, interference, and unauthorized access, including where such controls are implemented by third-party hosting or cloud service providers.	Power cable protection practices MUST ensure that: a) power cables are segregated from communications cabling where feasible b) cabling is installed in a manner that reduces risk of damage or interference (e.g., concealed routing) c) inspection and termination points are secured d) alternative routing or feeds are implemented to improve resilience e) exposure of cabling through public or unsecured areas is minimized	M	U
HST11.11	The vendor MUST ensure that the power supply to highly sensitive facilities is protected and resilient to disruptions, including where such controls are implemented by third-party hosting or cloud service providers.	Power supply protection practices MUST ensure that: a) uninterruptible power supply (UPS) is implemented to support orderly shutdown of systems b) surge protection mechanisms are in place c) backup power sources (e.g., generators) are available for extended outages d) emergency lighting is available during power failures e) emergency power-off mechanisms are accessible and appropriately located	M	U
HST11.12	The vendor MUST ensure that their information systems are deployed in locations that meet the vendor-	Environmental control practices MUST ensure that: a) system environments meet vendor-defined requirements for temperature, humidity, and air quality	M	R

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	specified requirements for cooling, heating, humidity and air quality.	b) environmental conditions are continuously monitored c) alerts are generated for deviations outside acceptable thresholds d) environmental controls are maintained to prevent system degradation or failure		
HST11.13	The vendor MUST ensure that telecommunications cabling supporting the hosted EMR Offering is protected from interception, damage, and unauthorized access, including where such controls are implemented by third-party hosting or cloud service providers.	Telecommunications cabling protection practices MUST ensure that: a) Installation of armoured conduit and locked rooms or boxes at inspection and termination points b) Use of alternative routings and/or transmission media c) Use of fibre optic cabling d) Use of electromagnetic shielding to protect the cables e) Placement of redundant links f) Initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables g) Controlled access to patch panels and cable rooms.	M	U
HST11.14	The vendor MUST ensure that telecommunications equipment is connected to the utility provider by at least two diverse routes to prevent connection failures, including where such controls are implemented by third-party hosting or cloud service providers.	Telecommunications resilience practices MUST ensure that: a) connections to utility providers are established through diverse routes b) redundancy is implemented to prevent single points of failure c) routing diversity is regularly assessed for effectiveness	M	U
HST11.15	The vendor MUST ensure that highly sensitive facilities are protected from natural and man-made hazards (e.g., in an area with a low risk of flooding, fire, explosion, or damage from neighbouring activities), including where such controls are implemented by third-party hosting or cloud service providers.	Facility location risk practices MUST ensure that: a) facilities are located in areas with reduced exposure to natural and man-made hazards b) risk assessments consider environmental and neighbouring threats c) mitigation strategies are implemented for identified risks	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST11.16	The vendor MUST minimize the impact of hazards in highly sensitive facilities, including where such controls are implemented by third-party hosting or cloud service providers.	Hazard mitigation practices MUST ensure that: a) fire suppression equipment is readily accessible b) personnel are trained in emergency response procedures c) environmental conditions such as temperature and humidity are monitored and controlled d) response capabilities are in place to address minor incidents promptly	M	U
HST11.17	The vendor MUST ensure that fire alarms in highly sensitive facilities are monitored continuously, tested regularly and serviced in accordance with manufacturer specifications, including where such controls are implemented by third-party hosting or cloud service providers.	Fire detection practices MUST ensure that: a) fire alarms are continuously monitored b) fire detection systems are tested at defined intervals c) systems are maintained in accordance with manufacturer specifications d) maintenance and testing activities are documented	M	U
HST11.18	The vendor MUST ensure that existing data centre facilities, and those being acquired by lease, purchase, or construction, are periodically assessed to ensure that physical security controls are in place to physically protect the information stored or processed in that data centre.	Data centre assessment practices MUST ensure that: a) facilities are periodically assessed for adequacy of physical security controls b) assessments consider protection of information and supporting systems c) deficiencies are identified and remediated d) assessments are documented and reviewed	M	U
HST11.19	The vendor data centre facilities MUST be separated into distinct areas depending on operational requirements (e.g., server rooms, wiring closets, call centres, system support areas, service delivery,	Facility zoning practices MUST ensure that: a) data centre areas are defined based on operational requirements b) each area is assigned a physical security zone	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	receiving, etc.).	c) security controls are applied based on zone classification d) zoning aligns with Appendix G: Physical Security Zones		
HST11.20	The vendor MUST layer physical security zones in data centres to provide for Defense in Depth (DiD) protection. If such an approach is not feasible (e.g., due to the physical layout of a particular environment or specific operational requirements), any deviation from layered zoning MUST be risk-assessed through a Threat and Risk Assessment (TRA), and compensating controls MUST be investigated and implemented.	Defense-in-depth practices MUST ensure that: a) multiple physical security zones are implemented to provide layered protection b) zone design minimizes direct access to highly sensitive areas c) deviations from layered zoning are risk-assessed d) compensating controls are implemented where zoning constraints exist	M	U
HST11.21	The vendor MUST ensure that physical access points in data centres, such as delivery and loading areas and other points where unauthorized persons may enter the premises MUST be controlled and, if possible, isolated from areas that house highly sensitive information systems to avoid unauthorized physical access.	Access point control practices MUST ensure that: a) physical access points are controlled and monitored b) high-risk entry points (e.g., loading areas) are secured c) access points are isolated from sensitive areas where feasible d) unauthorized access risks are minimized through design and controls	M	U
HST11.22	The vendor MUST require all agents and electronic service providers to obtain written approval from one of the vendor's senior-level executives	Asset removal practices MUST ensure that: a) removal of information technology assets requires formal approval b) approvals are obtained from authorized senior personnel	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	before leaving the data centre premises with information technology that is necessary for the operation of their information systems (e.g., servers and network devices). A written record of all assets removed off-site should be maintained.	c) all removed assets are recorded and tracked d) asset movement is documented for audit and accountability purposes		

11. Supplier and Third-Party Management

These requirements define controls for managing third parties and sub-processors, including security, privacy, and contractual obligations to ensure consistent protection of information and services, and to support ongoing assurance and oversight throughout the EMR Vendor relationship.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST12.01	The EMR Vendor MUST identify electronic service providers and categorize them by supplier type and the criticality of the services they provide.	Third-party classification practices MUST ensure that: a) Electronic service providers are identified and categorized by supplier type (e.g., application, network, storage, infrastructure, support services) b) Suppliers are assessed and classified based on the criticality and sensitivity of the services they provide, including their impact on PHI, system availability, and security c) Classification criteria are defined and applied consistently across all service providers d) Supplier classifications are reviewed and updated periodically or upon changes to services, risk, or contractual scope	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST12.02	The EMR Vendor MUST maintain formal documentation of the technical, organizational, and contractual relationships with electronic service providers.	Third-party documentation practices MUST ensure that: a) Technical and organizational relationships clearly define roles and responsibilities under PHIPA and applicable privacy and information security policies and procedures b) Roles and responsibilities for implementing, maintaining, and supporting information systems or services are documented and assigned c) Service characteristics and expectations are defined, including: i. The level of criticality of the service ii. The dates and times when the service is required iii. Capacity requirements of systems and networks iv. Maximum permissible downtime and service level objectives v. Service level reporting requirements and frequency vi. Critical timescales beyond which service disruption is unacceptable vii. Remedies or penalties in the event of failure to meet agreed service levels or obligations d) Expected deliverables and obligations of electronic service providers are documented e) Designated representatives and points of contact for each electronic service provider are identified f) Minimum information security and privacy controls applicable to the service provider are defined and enforced	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		g) Documentation is maintained in formal agreements (e.g., contracts, service agreements, service level agreements) and kept current		
HST12.03	The EMR Vendor MUST assess the potential information security and privacy risks posed by electronic service providers to the EMR Vendor prior to engaging in a contractual relationship with that electronic service provider.	Third-party risk assessment practices MUST ensure that: a) Risk assessments evaluate the impact of the service provider on PHI, system security, availability, and regulatory compliance b) Assessments consider the type of service, data access, data sensitivity, and level of integration with the EMR environment c) Due diligence includes review of the service provider's security posture (e.g., certifications, controls, policies, incident history) d) Identified risks are documented and addressed through mitigation measures, contractual controls, or risk acceptance processes e) Risk assessments are reviewed and updated where there are significant changes to the service, scope, or risk profile	M	U
HST11.04	The EMR Vendor MUST define and document all information systems and services to be provided by electronic service providers, including for new engagements and renewals, within formal service agreements.	Third-party service agreement practices MUST ensure that: a) Roles and responsibilities under PHIPA and applicable privacy and information security policies and procedures are clearly defined b) Roles and responsibilities for implementing, maintaining, and supporting the information systems or services are documented c) Service characteristics and expectations are defined, including: viii. The level of criticality of the service	M	R

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		ix. The dates and times when the service is required x. Capacity requirements of systems and networks xi. Maximum permissible downtime and service level objectives xii. Service level reporting requirements and frequency xiii. Critical timescales beyond which service disruption is unacceptable xiv. Remedies or penalties in the event of failure to meet agreed service levels or obligations h) Minimum information security and privacy controls applicable to the service provider are defined and enforced		
HST12.04	The EMR Vendor MUST establish and implement a consistent process for managing the termination of electronic service provider relationships.	Third-party termination practices MUST ensure that: a) Roles and responsibilities are defined for managing the termination process b) Physical and logical access rights to systems, data, and facilities are revoked in a timely manner c) All assets are securely returned, transferred, or destroyed, including data, backup media, documentation, hardware, and authentication devices d) Data held by the electronic service provider is returned to the EMR Vendor or securely disposed of in accordance with contractual ownership terms, retention requirements, and applicable privacy obligations e) Termination activities are documented and validated to ensure completeness	M	U

12. Compliance and Assurance

These requirements define controls for compliance and assurance, including risk assessment, independent verification, and evidence submission to demonstrate adherence to applicable legal, regulatory, and contractual obligations.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST13.01	The EMR Vendor MUST provide evidence of formal alignment with, or certification against, recognized international security and cloud-specific frameworks for the application and its hosting environment.	EMR Vendor MUST provide evidence to show the following industry-standard frameworks or equivalent frameworks: a) Provide a valid ISO/IEC 27001 certificate (and ISO 27017 cloud extension if available) covering the EMR application and operations. b) Provide documentation (such as a mapping or CAIQ) demonstrating adherence to NIST SP 800-53 Rev. 5 and CSA CCM v4 domains. c) Include the equivalent security certificates from the underlying Cloud Infrastructure Provider (e.g., AWS, Azure, or GCP).	O	N
HST13.02	The EMR vendor MUST provide a current SOC 2 Type 2 report (covering Security, Availability, and Confidentiality) conducted by an independent third-party audit firm.	A SOC Type 2 report is required to prove that the security controls were tested and remained effective over a specified period. a) If the most recent SOC 2 report is older than six months, the vendor must provide a signed "Bridge Letter" (Letter of Comfort) confirming that no material changes have occurred in their control environment since the last audit. b) The report must include the vendor's subprocessors (e.g., AWS or Azure) to ensure the entire hosting chain is covered.	O	N
HST13.03	The EMR Vendor MUST require an electronic service provider to implement all applicable information security and privacy controls prior to the electronic service provider being granted access to the hosted EMR Vendor.	Third-party onboarding practices MUST ensure that: a) Applicable security and privacy controls are defined and communicated to the electronic service provider prior to access b) Implementation of required controls is validated before granting access (e.g., attestations, assessments, or evidence of compliance) c) Access is not provisioned until required controls are in place and approved d) Control requirements are aligned with the sensitivity of data and criticality of the service	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST1.06	The EMR Vendor MUST ensure that threat risk assessments are performed on their electronic service providers.	a) Third-party risk management practices MUST ensure that: a) Threat and risk assessments evaluate potential threats, vulnerabilities, and impacts associated with the electronic service provider b) Assessments consider the nature of the service, data sensitivity (including PHI), system access, and integration with the EMR environment c) Assessments are conducted prior to onboarding and periodically thereafter based on risk and criticality d) Identified risks are documented and addressed through mitigation measures, contractual controls, or risk acceptance processes e) Assessment results are reviewed and updated when there are changes to the service, scope, or threat landscape	M	R
HST13.04	The EMR Vendor MUST establish contingency arrangements to ensure that business processes can continue in the event that an electronic service provider is unavailable.	Third-party continuity practices MUST ensure that: a) Contingency arrangements are based on the results of threat and risk assessments b) Alternative, secure facilities or service providers are available to support continuity of critical business processes c) Escrow arrangements are established, where applicable, for critical assets or proprietary technologies (e.g., application source code, cryptographic keys) using a trusted third party d) Recovery arrangements are in place to ensure continued availability of information stored with the service provider or in cloud environments e) Contingency arrangements are aligned with the EMR Vendor's business continuity and disaster recovery programs	M	U

13. APPENDICES

13.1 Appendix A: Glossary

TERM	DEFINITION
All persons	The EMR Vendor, including its staff, agents, suppliers and electronic service providers.
Hardware Security Module (HSM)	A physical or virtual cryptographic device used to securely generate, store, protect, and manage cryptographic keys and perform encryption-related operations.
Intrusion Detection and Intrusion Prevention Systems (IDS/IPS)	Security technologies used to monitor, detect, alert on, and/or prevent unauthorized, malicious, or suspicious activity within networks or systems.
Key Management Service (KMS)	A cloud-hosted or externally managed service used to centrally manage cryptographic keys, encryption operations, and key lifecycle activities within hosted or hybrid environments.
Message Authentication Code (MAC)	A cryptographic value used to verify the integrity and authenticity of a message or data using a shared secret key.
Privileged ID	A user account that has more privileges than ordinary users. Privileged accounts might, for example, be able to install or remove software, upgrade the operating system, or modify system or application configurations.
Service ID	An account in the EMR Vendor, with elevated privileges, that is managed by The EMR Vendor. A unique identifier assigned to a non-human account used by an application, service, or process to perform automated actions within a system.
System ID	A unique identifier assigned to an information system or application for the purpose of identification and authentication in system-to-system interactions.
Interactive Login	A user-initiated authentication that establishes a direct session with a system (e.g., via UI, console, or remote access).
IoT	IoT (Internet of Things) refers to network-connected medical and operational devices that collect, exchange, or transmit data to support clinical care, monitoring, automation, and healthcare operations.
User ID (managed by vendor)	Credentials within the EMR Vendor that are managed by The EMR Vendor.

13.2 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).
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

	Personal IDs & Privileged IDs	Service IDs
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.

13.3 Appendix C: Information Security Incident Management

Part 1: Incident Severity and Priority Ratings

- Severity Ratings

Severity	Category and Description	Recommended Maximum Time Frames		
		Triage	Containment	Recovery
1	Critical - Critical or multiple sites down - Loss of service poses a substantial risk to participating HICs - Posing a public health safety, privacy or security risk - Causing significant adverse impact affecting a large number of internal and/or external systems, e.g., large-scale malware outbreak Immediate response and restore – “all hands on deck”.	30 minutes	4 hours	12 hours
2	High - Single, critical site down - Loss of non-mission-critical service - Help desk unavailable - Service degradation affecting HICs Response/restore as quickly as possible - within one business day	2 hours	8 hours	24 hours
3	Medium - Application or physical component slow-downs - Minor technical or functional problems - Application or component failure affecting a single client Restore within the next few business days	4 hours	36 hours	48 hours

Severity	Category and Description	Recommended Maximum Time Frames		
		Triage	Containment	Recovery
4	Low Minimal impact, not time-critical, or workaround exists Restore within a week	24 hours	48 hours	7 days

Part 2: Incident Severity and Priority Ratings

- Priority Ratings

Incident Type	Priority Rating	
	P2	P1
Access control: Reserved for security incidents related to a potential compromise of access control		
Privilege account compromised E.g., a Privileged ID (such as system administrators, database administrators, or firewall administrators) demonstrates unusual activities/behaviours (e.g., unexplained logins, unexplained file accesses)		X
Phishing attack detected – targeting privileged users: E.g., numerous suspicious emails targeting users with privileged access		X
Asset security: For incidents that involve lost or stolen assets and attacks on an asset causing disruption of service		
Loss of unencrypted storage media E.g., loss of an unencrypted USB drive containing sensitive data is lost	X	
Denial of Service (DoS) attack against a critical asset detected E.g., a DoS attack initiated against a server hosting business-critical applications		X
Data security: For incidents that threaten the confidentiality of data		

Incident Type	Priority Rating	
	P2	P1
An unusually high volume of data access on server(s) hosting sensitive data/applications that process or store sensitive data E.g., a system alarm is triggered that there is a high volume of data transfer during non-business hours (not caused by data backup)	X	
Malware / Virus infection detected– high impact E.g., an alarm is triggered that a virus outbreak has been detected		X
Data and System Integrity: Incidents related to a potential compromise of the integrity of data or systems		
A major data breach that has attracted media attention: E.g., a major data breach of any kind		X
Tape backup failed over a period of time E.g., a tape backup failed for the past five sessions	X	

Part 3: Incident Report Details

The following details are required in an information security incident report:

1. Contact Information of the EMR user, agent or electronic service provider that reported the incident, AND the incident response lead or team
 - a) Name
 - b) Unit (e.g., department, division, team) (if applicable)
 - c) Email address
 - d) Phone number
 - e) Location (e.g., mailing address, building and room number)

2. Incident Details

- f) Date/time when the incident was discovered
- g) Estimated date/time when the incident started
- h) Incident ticket number
- i) Type of incident (e.g., denial of service, malicious code, unauthorized access, inappropriate usage)
- j) The physical location of the incident (e.g., city,)
- k) Current status of the incident (e.g., ongoing attack)
- l) Source/cause of the incident (if known), including hostnames and IP addresses
- m) Description of the incident (e.g., how it was detected, what occurred)
- n) Description of affected resources (e.g., networks, hosts, applications, data), including information systems' hostnames, IP addresses, and function
- o) The operating system, version, and patch level
- p) Antivirus software installed, enabled, and up-to-date (yes/no)
- q) Mitigating factors
- r) Estimated technical impact of the incident (e.g., data is deleted, the system crashed, application unavailable)
- s) Actions performed by the agent or electronic service provider who reported the incident (e.g., shutting down the host, a disconnected host from the network)
- t) Other organizations contacted (e.g., software vendor)
- u) Type of information compromised (if applicable)
- v) General Comments
- w) Summary of the Incident
- x) Contact information for all involved parties
- y) Log of containment/mitigation actions taken by incident response lead/team
- z) List of evidence gathered
- aa) Cause of the Incident (e.g., misconfigured application, unpatched host)
- bb) List of recommended and implemented remediation activities
- cc) Current Status of the Incident Response

13.4 Appendix D: 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.

13.5 Appendix E: Security Logging and Monitoring

Sources and Contents of Logs

System/Software	Event/Activity to be Recorded
Anti-malware software (E.g., anti-virus, anti-spyware and rootkit detectors)	• Instances of detected malware • File and information system disinfection attempts • File quarantines • Malware scans • Signature or software updates
Intrusion detection and intrusion prevention systems	• Suspicious behaviour • Detected attacks • Actions performed to stop malicious activity
Remote access and wireless access systems	• Login attempts • Amount of data sent and received during a session
Web proxies	URLs accessed
Vulnerability Management Software (includes patch management and vulnerability assessment software)	• Patch installation history • Vulnerability status • Known vulnerabilities • Missing software updates
Authentication Servers (includes directory servers and single sign-on servers)	Authentication attempts
Routers and switches	Blocked activity
Firewalls	Detailed logs of network activity

System/Software	Event/Activity to be Recorded	
Network Quarantine Servers	• Status of host security checks • Quarantined hosts and reason	
Identity Provider Services	Reference the Log Generation section of this Security Logging and Monitoring standard and the Federation Identity Provider Standard	
Data Contribution Endpoints	Reference the Log Generation section of this Security Logging and Monitoring standard	
Operating Systems (such as those for servers, workstations and networking devices (e.g., routers, switches))	• System Events • System shut down • Service starting	• Security Events • File accesses • Policy changes • Account changes
Applications (e.g., e-mail servers and clients, Web servers and browsers, file servers and file-sharing clients, database servers, etc.) * Note: Refer to the Error! Reference source not found. section for EMR Offering application-level (PHI) logging and auditing requirements.	• Client requests and server response • Authentication attempts • Account changes • Use of privileges • Number and size of transactions • Operational events • Start-up and shutdown	• Configuration changes • Application-specific events such as: • Email sends and receipts • File access • Service request • System-level transactions • A function performed (such as read, write, modify, delete)

13.6 Appendix F: Information Asset Management

Part 1: Information and Asset Classification Scheme

Classes		Description	Examples of Information or Assets	Examples of Risk Impacts
Confidentiality	Integrity and Availability			
Public	LOW	Information or assets that are used in the normal course of business and that is unlikely to cause harm Available to public	- Information found on the externally hosted EMR Vendor website - External job postings	- No impact if made publicly available - If lost, would not result in injury to patients, the hosted EMR Vendor or its agents or electronic service providers, or HICs, their agents or electronic service providers - Loss of integrity or availability does not have an adverse impact on patients, the hosted EMR Vendor, its agents or electronic service providers, or HICs, their agents or electronic service providers
Internal	LOW	Information or assets that have a low sensitivity outside of the hosted EMR Vendor and could have low levels of impact on service levels or performance, or result in low levels of financial loss Available to all agents of the hosted EMR Vendor and electronic service providers of the hosted EMR Vendor and HICs with a need-to-know	- User manuals for the hosted EMR Vendor applications - High-level hosted EMR Vendor planning documents - High-level financial information concerning the effective operation of the hosted EMR Vendor	- Low degree of risk if made publicly available - Loss of integrity or availability may have minimal adverse impact on patients, the hosted EMR Vendor, its agents or electronic service providers, or HICs, their agents or electronic service providers

Classes		Description	Examples of Information or Assets	Examples of Risk Impacts
Confidentiality	Integrity and Availability			
Confidential	MEDIUM	Information or assets that have a moderate to high sensitivity within the hosted EMR Vendor and outside of the hosted EMR Vendor and could have a moderate impact on service levels or performance, or result in moderate levels of financial loss Available only to a specific function, group or role in the hosted EMR Vendor, its agents or electronic service providers or HICs, their agents or electronic service providers	- Personal information (not including PHI), e.g., an identifiable agent's rate of pay - Information covered by non-disclosure agreements - Financial transactions that do not include PHI or Restricted information - Detailed network architecture documents	- Loss of reputation - Loss of confidence in the hosted EMR Vendor - Loss of personal privacy - Loss of trade secrets or intellectual property - Loss of integrity or availability may have a moderate adverse impact on patients, the hosted EMR Vendor, its agents or electronic service providers, or HICs, their agents or electronic service providers
PHI	HIGH	All PHI Available only to a specific function, group or role in the hosted EMR Vendor, its agents or electronic service providers or HICs, their agents or electronic service providers	PHI	- Loss of reputation - Loss of personal health information privacy - Loss of confidence in the hosted EMR Vendor - Loss of integrity or availability may have moderate to serious adverse impact on a patient, the hosted EMR Vendor, its agents or electronic

Classes		Description	Examples of Information or Assets	Examples of Risk Impacts
Confidentiality	Integrity and Availability			
				service providers, or HICs, their agents or electronic service providers
Restricted	CRITICAL	Information or assets that are extremely sensitive, both inside and outside of the hosted EMR Vendor, could have a high impact on service levels or performance or result in high levels of financial loss Available only to named individuals or specified positions. (e.g., John Doe or Vice-President of Operations), in the hosted EMR Vendor, its agents or electronic service providers or HICs, their agents or electronic service providers	• Cryptographic Keys • Passwords • Hardware Security Modules	• Loss of reputation • Significant financial impact • Loss of significant amounts of personal health information privacy • Loss of confidence in the hosted EMR Vendor • Destruction of partnerships and relationships • Loss of integrity or availability may have a serious to extreme adverse impact on patients, the hosted EMR Vendor, its agents or electronic service providers, or HICs, their agents or electronic service providers

Part 2: Information and Asset Labeling

	Media Type	Public	Internal	Confidential	PHI	Restricted
Paper Material	Optional		Must be labelled on the first page, and each subsequent page			
Electronic Information	Optional		Must be labelled on the first page, and each subsequent page of any electronic information capable of being printed (e.g., screen capture, PDF, word processing document, spreadsheet, slide show presentation, etc.)			
Email	Optional		Must be labelled in the body or subject			
Portable Removable Media	Optional					
Integrated Storage Device	Optional					

Part 3: Information and Asset Handling Protection Requirements - Storage Requirements

Information/ Asset Type	Public	Internal	Confidential	PHI	Restricted
Paper material	No special confidentiality, integrity, or availability requirements	Locked in storage container left unsupervised in areas with access to the public - OR - Stored in an area that can only be accessed by The EMR Vendor, its agents or electronic service providers	Locked in a storage container if left unsupervised in areas with access to the public or unauthorized persons - OR - Stored in an access-controlled area in which all with access are authorized to view the information	Locked in a storage container if left unsupervised in areas with access to the public or unauthorized persons - OR - Stored in an access-controlled area in which all with access are authorized to view the information	Must be held under dual control and split knowledge Audit trail kept for all physical access (e.g., a log of signatures maintained each time a person accesses the information) Must be stored in an access-controlled area AND locked in a storage container
Electronic Information	No special confidentiality, integrity, or availability requirements	Must be stored on an internal network or storage device	Must be stored on an encrypted device - OR - Stored on internal network storage that has logical controls to prevent unauthorized access	Must be stored on an encrypted device and only the minimum amount of PHI required must be stored - OR - Stored on encrypted internal network storage that has logical controls, and where applicable physical controls, to prevent unauthorized access	Must be stored on an encrypted device and only the minimum amount of Restricted information must be stored - OR - Stored on encrypted internal network storage that has logical controls, and where applicable physical controls, to prevent unauthorized access
Portable removable media	No special confidentiality, integrity, or	Must be stored in an access-controlled area	Must be encrypted	Must be encrypted	Must be encrypted

Information/ Asset Type	Public	Internal	Confidential	PHI	Restricted
	availability requirements		Must be locked in a storage container or access-controlled area when not in use or unsupervised	Must be locked in a storage container or access-controlled area when not in use or unsupervised	Must be stored in an access-controlled area AND locked in a storage container, when not in use or unsupervised Should be held under dual control The audit trail should be maintained for all physical access to the device
Integrated Storage Device	Should be stored in an access-controlled area Regular backups should be performed to ensure availability and integrity	Must be stored in an access-controlled area Regular backups should be performed to ensure availability and integrity	Should be encrypted Must be stored in an access-controlled area Regular backups must be performed to ensure availability and integrity	Must be encrypted Must be stored in an access-controlled area Regular backups must be performed to ensure availability and integrity	Must be encrypted Must be stored in a highly secured access-controlled area Must maintain an audit trail for physical access to the device Regular backups must be performed to ensure availability and integrity

13.7 Appendix G: Physical Security Zones

This table defines the physical security zones applicable to the EMR environment, including their characteristics and required controls. Zones MUST be established based on the sensitivity of information and systems, with each successive zone enforcing increased levels of access restriction, monitoring, and physical protection.

ZONES	DESCRIPTION	REQUIREMENTS
Public Zone	Any public entrance to a physical facility and the immediate environment around it is considered a public zone. Public zone examples include: • Facility parking lots • Grounds surrounding a facility • Any area of unimpeded public access during posted business hours.	Public zones SHOULD be subject to basic environmental awareness and monitoring where feasible, recognizing that direct control may be limited.
Reception Zone	A reception zone is an area where public access intersects with facility staff or operations for administrative reasons or to obtain access. Reception zone examples include: • The main entrance of a facility or a floor in shared accommodation situations; • Visitor receiving and waiting areas; and • Public service desks and kiosks.	• Physical access control must be in place to restrict further public movement (e.g., through the use of a reception desk, guards, or physical access devices, such as card readers). • Where possible, public/visitor access to the reception zone should be limited to specific hours (e.g., it may be limited in a data centre, but not in a hospital). • Any required authentication and approval for facility access (e.g., presentation of credentials or validation of authorized access) should take place within the reception zone.
Operations Zone	An operations zone is a periodically or informally monitored area within the facility where access is limited to authorized personnel and approved/escorted visitors only. Operation zone examples include: • Storage closets • Employee offices and similar areas	• Must have a recognizable perimeter. • Must not permit public access, and employ physical barriers (e.g., walls, locked doors etc.) for this purpose. • Must only be accessible via a reception zone, and separated from the reception zone by a wall and locking the door (unless subject to an exemption as per requirement 2.17 of this document).
Security Zone	A security zone is an area within the facility that is monitored continuously and is accessible to authorized personnel and approved/escorted visitors only.	• Must have a recognizable perimeter and employ robust, reliable high-effectiveness physical barriers to access; • Must be constructed such that all barriers and doors remain continuously closed and locked when not in use; • Must employ activity monitoring with an immediate response;

ZONES	DESCRIPTION	REQUIREMENTS
	The secure raised floor portion of a data centre is appropriate for inclusion within a security zone. Other areas of a facility (e.g., sensitive wiring closets) may also be defined as security zones.	• Access must be controlled and recorded at all times, e.g., through the use of a guard to gain entry or through the use of a card reader that records access; and • Must be located within an operations zone (unless subject to an exemption as per requirement 2.17).
High-Security Zone	A high-security zone is an area within the facility that is monitored continuously and is accessible only to a specific list of screened and authorized personnel or approved/escorted visitors accompanied by screened and authorized personnel. A dedicated, sensitive processing environment that must be physically separated from raised floor operations is appropriate for inclusion within a high-security zone.	• Must have a recognizable perimeter and employ robust, reliable high-effectiveness physical barriers to access. • Must be constructed such that all barriers and doors remain continuously closed and locked when not in use. • Must employ continuous activity monitoring with an immediate response. • All access must be controlled and recorded at all times and MUST be audited, at a minimum, monthly. • Persons who require access must successfully undergo screening and be added to a list or roster of authorized persons prior to being granted access. • All approved visitors must be accompanied at all times by a screened and authorized individual. • Must be located within a security zone (unless subject to an exemption as per requirement 2.17). • Controls must include mechanisms to detect and respond to physical tampering or unauthorized access attempts