

EMR Hosting

Requirements

July 4, 2024

Document Version & Status: 1.4 – Final



1. Table of Contents

1. TABLE OF CONTENTS	2
1. INTRODUCTION	3
1.1 PURPOSE.....	3
1.2 VERSION HISTORY.....	3
2. EMR SPECIFICATION SCOPE.....	4
3. EMR REQUIREMENTS	6
4. EMR HOSTING SECURITY REQUIREMENTS	14
4.1 NETWORK AND OPERATIONS	14
4.2 PHYSICAL SECURITY.....	21
4.3 ACCEPTABLE USE OF INFORMATION AND INFORMATION TECHNOLOGY.....	24
4.4 ACCESS TO CONTROL AND IDENTITY MANAGEMENT FOR SYSTEM-LEVEL ACCESS.....	28
4.5 INFORMATION AND ASSET MANAGEMENT.....	35
4.6 INFORMATION SECURITY INCIDENT MANAGEMENT.....	36
4.7 BUSINESS CONTINUITY	40
4.8 CRYPTOGRAPHY	43
4.9 SECURITY LOGGING AND MONITORING.....	49
4.10 ELECTRONIC SERVICE PROVIDER	52
5. APPENDICES.....	55
5.1 APPENDIX A: GLOSSARY	55
5.2 APPENDIX B: PHYSICAL SECURITY ZONES.....	55
5.3 APPENDIX C: MINIMUM PASSWORD REQUIREMENTS.....	58
5.4 APPENDIX D: INFORMATION ASSET MANAGEMENT.....	60
5.5 APPENDIX E: INFORMATION SECURITY INCIDENT MANAGEMENT.....	66
5.6 APPENDIX F: APPROVED CRYPTOGRAPHIC ALGORITHMS.....	70
5.7 APPENDIX G: SECURITY LOGGING AND MONITORING	74

1. INTRODUCTION

1.1 Purpose

The purpose of this document is to specify requirements for a vendor that hosts its EMR Offering. Hosting an EMR Offering refers to the business and technical services a vendor provides to make the EMR Offering remotely available over a wide area network (e.g., via the Internet). This specification defines the requirements and expectations for hosting an OMD-certified EMR Offering by a vendor.

For a hosted EMR Offering, the EMR application and data are hosted in a centralized location that the vendor is accountable for ensuring is protected and maintained. It is understood that vendors may use third-party electronic service providers to help them host the EMR Offering (e.g., contracting to third parties to provide data centres and infrastructure as a service).

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 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2017-08-04	a) Initial release
1.1	2019-10-10	a) Updated broken links. b) Updated references in Related Documents. c) Various typos, grammar, errata and cosmetic formatting issues. d) Removed Comments column (No content exists in them). e) Updated EMR21.01 to include PIA wording. f) Removed context about compliance for certification in section 5. g) Refined wording in section 1.1.1.
1.2	2021-01-25	a) Updated formatting for conformance with the current specifications template. b) Removed the Specification version in the document title.

VERSION	REVISION DATE	REVISION NOTES
1.3	2021-12-22	<ul style="list-style-type: none"> a) Updated references to Ontario Health (Digital Services), formerly eHealth Ontario. b) Moved the following requirements related to Privacy and Security Specification: <ul style="list-style-type: none"> i. Threat Risk Management (previously HST08.XX) c) Re-sequenced requirements: <ul style="list-style-type: none"> i. from HST09.XX to HST08.XX ii. from HST10.XX to HST09.XX iii. from HST11.XX to HST10.XX iv. from HST12.XX to HST11.XX d) Corrected various errata
1.4	2024-07-04	<ul style="list-style-type: none"> a) Separated business context and overview as a separate document b) Generalized terminology to apply to vendors beyond just EMR vendors c) Added Appendix H: Glossary to define terms used in this specification d) Added wording in the Network and Operations section for clarity on the audience to whom the requirements are applicable. e) Updated wording in the Hosted EMR Offerings section for clarity of the definition of a Hosted EMR Offering. f) Retired HST01.10, no longer relevant. Refer to EMR EHR Connectivity Specification for more information on EHR service connectivity g) Updated HST01.11 for clarity on how response times are measured and publication of summary reports on request. h) Updated HST02.35 for clarity of the responsible party i) Updated HST02.36 for clarity of the responsible party j) Retired HST04.34 and HST04.35, requirements are duplicates of HST04.04 and HST04.05 respectively.HST05.34 k) Updated HST06.06: Updated for clarity to secure confidential data

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
- Release Notifications
- Implementation Plan
- Training for Enhanced Use
- Business Continuity
- Data Recovery

- Accessibility
- Provincial EHR Solutions and Services Interoperability
- Service Levels

The EMR information security requirements expressed within this document are derived from eHealth Ontario's EHR information security policies, which are based on ISO 27002 control objectives, and cover the following topics:

- Network and Operations
- Physical Security
- Acceptable Use of Information and Information Technology
- Access to Control and Identity Management for System-Level Access
- Information Asset Management
- Information Security Incident Management
- Business Continuity
- Cryptography
- Security Logging and Monitoring
- Electronic Service Provider

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.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST01.01	<p>Central Monitoring</p> <p>The vendor MUST have a central monitoring service that continuously monitors, alerts and reports on the status, availability and performance of its data centre facility, servers, network, storage, database, security and the EMR Offering application.</p>	<p>The monitoring service MUST include:</p> <ul style="list-style-type: none"> Data centre facility monitoring of power outages Environmental controls and network provider service interruptions Server availability and performance (e.g., CPU, memory, network and disk) Network disruption that impacts availability and performance Storage capacity and disk input/output (I/O) Backup errors <p>Database Management System (DBMS), transaction rates and volume of data; and security events, including intrusion detection systems and critical security events.</p>	M	P
HST01.02	<p>Client Notification Service</p> <p>The vendor MUST have a notification and alerting service to communicate timely service management status and notifications, outage or error status on interfaces to Provincial EHR Solutions and Services and other interfaces, overall service outage, and notifications about disaster details that affect the delivery of an EMR Offering and services to its subscribers and EMR users.</p>	<p>The notification and alerting service will be used, at a minimum, to notify affected subscribers and EMR users of events impacting EMR Offering service delivery, including but not limited to:</p> <ul style="list-style-type: none"> a) Planned and unplanned outages b) Disaster events c) EMR Offering availability and performance d) Availability and performance of operational Provincial EHR Solutions and Services e) General service notifications and reminders <p>The vendor MUST be able to send alerts and notifications using various methods such as but not limited to:</p> <ul style="list-style-type: none"> a) Email b) Telephone c) Web-based d) Mobile device message 	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		e) Fax EMR Offering messaging service		
HST01.03	Help Desk The 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 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	P
HST01.04	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.	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) 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.)	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		<ul style="list-style-type: none"> f) Known issues or limitations of the upgrade, e.g., a known bug, etc. g) Contact information for support h) Other resources and links <p>The following information is also helpful to include:</p> <ul style="list-style-type: none"> a) Troubleshooting b) Frequently Asked Questions (FAQs) 		
HST01.05	<p>Implementation Plan</p> <p>The vendor MUST publish implementation and upgrade plans to all affected subscribers and EMR users prior to:</p> <ul style="list-style-type: none"> a) The initial implementation of their EMR Offering; and b) Any subsequent update of their EMR Offering. 	<p>An implementation or upgrade plan MUST include at a minimum:</p> <ul style="list-style-type: none"> 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) <p>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:</p> <ul style="list-style-type: none"> a) roles and responsibilities of all parties b) a schedule c) vendor's approach to the migration of data <p>endor services related to data preparation, data migration and subsequent subscriber acceptance</p>	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST01.06	<p>Training for Enhanced Use</p> <p>vendor's training services made available to its subscribers and EMR users MUST include:</p> <ul style="list-style-type: none"> 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. 	<p>In addition to training on the standard features and functionality for an EMR Offering, the 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).</p> <p>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.</p>	M	P
HST01.07	<p>Business Continuity</p> <p>A business continuity plan for the hosted EMR Offering MUST be published by the vendor to its subscribers which describes the processes that will be followed and the services that will be available to the subscribers to continue the operation of their medical practices in the event of unplanned outages of their hosted EMR Offering.</p>	<p>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:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> I. Offline and read-only access to patient files II. Access to daily schedules by users III. Recording of patient encounters by users 	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		IV. Updating and synchronizing records as applicable once the operation of an EMR Offering has been restored.		
HST01.08	<p>Data Recovery</p> <p>A point-in-time recovery (PITR) solution MUST be implemented by the vendor that allows the EMR Offering Database Management System (DBMS) to be restored up to the point of failure.</p>	<p>The DBMS MUST implement features such as write-ahead transaction logs that can be used to replay all database transactions from the point of the last database backup to restore the EMR Offering up to the point of failure.</p>	M	P
HST01.09	<p>Accessibility</p> <p>EMR users in a medical practice MUST be able to access their EMR Offering:</p> <ul style="list-style-type: none"> a) From multiple physical locations using two or more client platform technologies; and b) Using an Internet browser or remote desktop solution. 	<p>EMR users may require access to their EMR Offering from several physical locations including, but not limited to:</p> <ul style="list-style-type: none"> a) Their designated primary medical practice location b) A satellite office c) A hospital d) Other remote locations <p>Client platform technologies include:</p> <ul style="list-style-type: none"> a) Microsoft Edge b) Apple iOS (Mac) c) Mobile device (e.g., smartphone or tablet) <p>The EMR Offering MUST be accessible using at least one of the following:</p> <ul style="list-style-type: none"> a) Microsoft Internet Explorer b) Mozilla-Firefox c) Google-Chrome d) Apple-Safari e) Remote Desktop Solution (e.g., Citrix Systems Inc.) 	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
HST01.10	<p>Provincial EHR Solutions and Services Interoperability</p> <p>An EMR Offering MUST be able to interoperate with operational Provincial EHR Solutions and Services according to the following architectural principles:</p> <p>(a) Service Orientated Architecture (SOA) using standardized messaging; and</p> <p>(b) Exchange of authentication and authorization data using OAuth2.0 as a basis for enabling single sign-on.</p>	<p>Background:</p> <p>The EMR Offering MUST be able to support Service Orientated Architecture (SOA). This requirement is a notice that an EMR Offering's interoperability with operational Provincial EHR Solutions and Services is a fundamental requirement for enabling the enhanced use of EMR Offerings by subscribers and EMR users.</p> <p>As an underlying architectural requirement, the EMR Offering MUST be able to interoperate with operational Provincial EHR Solutions and Services that are based on various Web Services standards and Transport Layer Interoperability (TLI) specifications to both consume and contribute data.</p> <p>Interoperating with these Provincial EHR Solutions and Services will also require ongoing alignment with messaging and terminology standards such as HL7, ICD-10-CA, SNOMED CT, etc.</p> <p>The specific requirements will be interface-specific and published over time by the interface authority.</p> <p>The EMR Offering MUST be able to support OAuth2.0.</p> <p>This requirement is a notice that support for OAuth2.0 is an underlying architectural requirement for enabling single sign-on support with Provincial EHR Solutions and Services.</p>	M	Retired
HST01.11	Service Levels	The EMR Offering MUST provide $\geq 99.9\%$ availability to subscribers per calendar month (excluding scheduled downtime).	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	<p>The hosted EMR Offering MUST be highly available, and meet requirements for system performance and Help Desk services.</p>	<p>The time to complete the following MUST be ≤ 3 seconds for 90% of occurrences, per calendar month:</p> <ul style="list-style-type: none"> 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 <p>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.</p> <p>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).</p> <p>Service-level summary reports MUST be provided upon request.</p>		

4. EMR HOSTING SECURITY REQUIREMENTS

4.1 Network and Operations

All requirements are mandatory for vendors and their hosted EMR Offering. The vendor and its hosted EMR Offering **MUST** have the functionality or provide the service described in the requirement. Requirements pertaining to the vendor also apply to additional parties the vendor may use to host an EMR and are often referred to as agents (i.e., anyone acting on behalf of the vendor), suppliers (i.e., anyone that provides goods or services to the vendor), and electronic service providers (i.e., a supplier that provides goods or services to enable a Health Information Custodian to use electronic means to collect, use, modify, disclose, retain or dispose of Personal Health Information). This includes the EMR Offering as an application and any hosting infrastructure to which individuals have access.

Referenced Policies:

- **eHealth Ontario Connecting Privacy Committee (CPC) Data Retention Policy.** This policy will be provided to vendors by OMD upon request until it is published by Ontario Health (Digital Services) here: <https://ehealthontario.on.ca/en/our-privacy-commitment>.

OMD #	REQUIREMENT	M/O	STATUS
HST02.01	<p>The vendor MUST maintain an inventory of all their physical information technologies that comprise the hosted EMR Offering. The inventory of assets MUST include, but is not limited to:</p> <ul style="list-style-type: none"> a) Type of asset, b) Information technology owner, where applicable c) Location of the information technology (and information technology owner, where applicable) d) Backup information. 	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST02.02	<p>The vendor MUST document and maintain network diagrams of all direct connections to the hosted EMR Offering. Network diagrams should include:</p> <ul style="list-style-type: none"> a) Physical and logical topologies b) Network device configuration c) Gateways to external networks d) Connected network devices 	M	P
HST02.03	The vendor MUST document and maintain operating procedures for the hosted EMR Offering. The operating procedures should specify the instructions for the detailed execution of jobs, such as performing backups, system restart and recovery procedures, and error handling.	M	P
HST02.04	The vendor MUST restrict all access to system documentation and operating procedures based on the principles of least privilege and need-to-know.	M	P
HST02.05	<p>The vendor MUST implement network zones and manage these network zones in a manner that observes the separation of different computing environments. The segregation of networks should be based on criteria, such as:</p> <p>The classification of information transmitted on the network, The level of assurance required.</p>	M	P
HST02.06	The vendor MUST ensure that networks are segregated, logically or physically, between the hosted EMR Offering, subscriber, information systems, and public networks.	M	P
HST02.07	The vendor MUST control traffic between network zones by using a security gateway at its network perimeter.	M	P
HST02.08	The vendor MUST configure their security gateways to filter traffic between network zones by denying all network traffic (inbound or outbound) by default and fail securely where availability requirements permit.	M	P
HST02.09	<p>The vendor MUST implement a process to review security gateway configurations at least annually. The process MUST ensure the:</p> <p>Review of the rule sets on their security gateways Removal of expired or unnecessary rules</p>	M	P

OMD #	REQUIREMENT	M/O	STATUS
	Resolution of conflicting rules Removal of unused or duplicate objects, e.g., network or computer systems.		
HST02.10	The 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.	M	P
HST02.11	The vendor MUST ensure that all connectivity to the hosted EMR Offering is secured to ensure the confidentiality and integrity of PHI that is transmitted (e.g., through the use of Transport Layer Security (TLS), virtual private network (VPN) tunnels, terminal services, etc.).	M	P
HST02.12	The vendor MUST require the hosted EMR Offering approved identifier (e.g., digital certificate, MAC address, IP address) to be used to indicate whether a data contribution end-point or identity provider service asset is permitted to connect to the network and which network zone the asset is permitted to connect. Considerations should be made for other assets connecting to the hosted EMR Offering.	M	P
HST02.13	The vendor MUST disable all unnecessary services, protocols, and ports on their information systems. The vendor should document and maintain justification for the use of all services, protocols, and ports allowed, including security features implemented for services, protocols, and ports considered to be insecure (e.g., FTP, Telnet, POP3, IMAP, and SNMP). The vendor should reference vendor specifications and industry benchmarks such as the Center for Internet Security (CIS).	M	P
HST02.14	The hosted EMR Offering MUST terminate all direct inbound and outbound external connections in a semi-trusted network zone (e.g., a demilitarized zone (DMZ)).	M	P
HST02.15	The hosted EMR Offering MUST ensure that all information system components that store information classified as internal or higher are located in an internal network zone, segregated from the DMZ and other untrusted networks.	M	P
HST02.16	The hosted EMR Offering MUST disable split tunnelling on any information system or information technology with access to the hosted EMR Offering, except for networking devices (e.g., routers, firewalls).	M	P
HST02.17	The hosted EMR Offering MUST harden all their information systems prior to implementation into the production environment.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST02.18	The hosted EMR Offering MUST remove all unnecessary functionality (e.g., such as drivers, features, subsystems, file systems, and unnecessary web servers).	M	P
HST02.19	The hosted EMR Offering MUST implement information security features for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).	M	P
HST02.20	The vendor MUST install firewall software on their agent's or electronic service provider's workstation, laptop, and where technically feasible other mobile devices, with direct connectivity to the Internet and the hosted EMR Offering.	M	U
HST02.21	The vendor MUST ensure that mobile workstations (e.g., notebooks, laptops, etc.) that have a documented business requirement to work with data extracts containing PHI have full-disk or partial encryption securely installed. Full disk encryption is the preferred method however containerized implementations of encryption on directories or specific locations are also acceptable. Implementations where PHI remains on managed servers in a protected data centre (e.g., Citrix) do not require encryption at rest.	M	P
HST02.22	The vendor MUST implement intrusion detection and prevention mechanisms (e.g., host intrusion detection/prevention systems and network intrusion detection/prevention systems) on their information systems and networks.	M	P
HST02.23	The vendor MUST protect their intrusion detection and prevention sensors (i.e., the hardware used to identify unauthorized activity in network traffic) against attack, for example, by using a network tap to hide the presence of the sensor.	M	P
HST02.24	The vendor MUST update intrusion detection and prevention software within defined timescales and at the recommendation of the vendor (e.g., upon the discovery of a server vulnerability).	M	P
HST02.25	The vendor MUST configure their intrusion detection and prevention software to provide an alarm or alert when suspicious activity is detected or prevented.	M	P
HST02.26	The vendor MUST configure thresholds for alarms and alerts to identify possible intrusion detection or prevention events, or violations of the hosted EMR Offering information security policies and its associated procedures.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST02.27	The vendor MUST respond to information security incidents identified by intrusion detection and prevention mechanisms in accordance with their information security incident handling process.	M	P
HST02.28	The vendor, its employees, agents and suppliers including electronic service providers MUST implement malware detection and repair software or equivalent solutions on all workstations (e.g., desktops, laptops) and servers. Alternative solutions may include application whitelisting or utilization of thin client implementations which restrict writable capabilities. Questions regarding the appropriateness of alternative solutions should be directed to OMD.	M	P
HST02.29	The vendor MUST ensure that virus definition files remain up-to-date.	M	P
HST02.30	The vendor MUST ensure all malware detection and repair software is up-to-date.	M	P
HST02.31	The vendor MUST program their malware detection and repair software to run at regular intervals, at a minimum weekly, unless scanning is performed in real-time. The vendor MUST disconnect infected information systems and information technology from the network until it has been verified that they are malware-free.	M	P
HST02.32	The vendor or their agent MUST implement malware detection and repair software to scan electronic or optical media, incoming files, electronic mail attachments, and downloads for malware before their use. These checks may be carried out at different places, such as electronic mail servers, and desktop computers.	M	P
HST02.33	The vendor or their agent MUST implement a vulnerability management process covering: a) Scanning and monitoring b) Risk assessment c) Remediation	M	P
HST02.34	The vendor or their agent MUST monitor their information systems to identify new vulnerabilities.	M	P
HST02.35	The vendor or their agent MUST perform vulnerability and configuration scans on the hosted EMR Offering, at a minimum, quarterly to determine the effectiveness of the implemented operational and technical security controls.	M	U

OMD #	REQUIREMENT	M/O	STATUS
HST02.36	The vendor or their agent MUST perform penetration tests, at a minimum annually, on all their Internet-facing applications that provide access to PHI to ensure that these applications do not expose the hosted EMR Offering to unknown threats.	M	U
HST02.37	Penetration tests on Internet-facing applications MUST include web-application testing techniques executed against a documented set of industry standards such as the Open Web Applications Security Project (OWASP) Top 10, to identify weaknesses that are unique to web-based applications (such as SQL/LDAP injection, cross-site scripting, session token attacks and URL forgery), and MUST be subject to rigorous external content review.	M	P
HST02.38	The vendor MUST ensure that all risks posed by identified vulnerabilities on their information systems and their remediation plans are assessed by a security analyst with independence from the operational teams.	M	P
HST02.39	The vendor MUST ensure that all vulnerabilities identified on their information systems are remediated within a defined timeline or MUST have the risk posed by the vulnerability formally accepted if the decision is made not to remediate.	M	P
HST02.40	The vendor MUST define timelines to react to the notification of potentially relevant vulnerabilities.	M	P
HST02.41	The vendor MUST implement a security patch management process to ensure that available patches are identified, assessed and, where feasible, deployed. The security patch management process may be a part of a general patch management process.	M	P
HST02.42	If a patch is available, the vendor MUST assess the risks associated with installing the patch (i.e., the risks posed by the vulnerability MUST be compared with the risk of installing the patch).	M	P
HST02.43	Where possible, the vendor MUST test and evaluate all patches prior to installation to ensure they are effective and do not result in side effects that cannot be tolerated.	M	P
HST02.44	If the decision is made not to patch, then the vendor MUST document the decision and make the appropriate conforming changes to inventory records and disaster recovery plans.	M	P
HST02.45	If no patch is available, or the decision is made not to patch, The vendor MUST consider implementing compensating controls to reduce the risks posed by the vulnerability. Controls may include:	M	P

OMD #	REQUIREMENT	M/O	STATUS
	a) Turning off services or capabilities related to the vulnerability b) Adapting or adding access controls (e.g., firewalls at the network border) c) Increasing monitoring to detect or prevent actual attacks		
HST02.46	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 and changing industry practices.	M	P
HST02.47	The vendor MUST ensure that all changes to networks and information systems follow their defined change control procedures.	M	P
HST02.48	The vendor MUST back up the hosted EMR Offering so that it may be recovered following a disaster or media failure.	M	P
HST02.49	At a minimum, the vendor MUST ensure that the EMR Offering is backed up in accordance with established and approved recovery time objectives (RTO) and recovery point objectives (RPO).	M	P
HST02.50	The vendor MUST ensure that backups are stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.	M	P
HST02.51	The vendor MUST secure all backups containing PHI. Encryption MUST be used when physically transferring data between sites.	M	P
HST02.52	The vendor MUST ensure that backup media and information systems are protected by physical and environmental controls equivalent to the physical and environmental controls applied at the main site.	M	P
HST02.53	The vendor MUST test backup media regularly and backup failures need to be tracked, reported and remediated.	M	P
HST02.54	The vendor MUST regularly test its restoration procedures to ensure that they are effective and that they can be completed within the time allotted in their operational procedures for recovery. At a minimum, restoration procedures MUST be tested annually.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST02.55	The retention period for data archives of the hosted EMR Offering shall be determined by the record retention requirements of the information they contain and in accordance with any legal or regulatory requirements (e.g., College of Physicians and Surgeons of Ontario).	M	P

4.2 Physical Security.

OMD #	REQUIREMENT	M/O	STATUS
HST03.01	The vendor MUST implement physical security perimeters to protect physical components of the hosted EMR Offering from unauthorized physical access and environmental damage.	M	P
HST03.02	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).	M	P
HST03.03	<p>The vendor MUST ensure that highly sensitive facilities (i.e., buildings or storage areas that house information systems that store or process PHI or Restricted information) are protected against unauthorized physical access. Methods for preventing physical access may include:</p> <ul style="list-style-type: none"> 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	P
HST03.04	The vendor MUST ensure that highly sensitive facilities are located away from areas that are easily accessible to the public. Details about highly sensitive facilities should be kept confidential (e.g., by using discrete signs or excluding details from directories or telephone books).	M	P
HST03.05	<p>The vendor MUST ensure that visitors to highly sensitive facilities are:</p> <ul style="list-style-type: none"> a) Permitted physical access only for specific, authorized purposes 	M	P

OMD #	REQUIREMENT	M/O	STATUS
	<ul style="list-style-type: none"> b) Monitored by recording arrival and departure times c) Obligated to wear visitor badges at all times d) Supervised at all times e) Made aware of behaviour or actions that are prohibited (e.g., filming or photography) 		
HST03.06	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).	M	P
HST03.07	<p>The vendor MUST ensure that power cables to highly sensitive facilities are protected. Methods of protection may include:</p> <ul style="list-style-type: none"> a) Segregating them from communications cables to prevent interference b) Concealed installation c) Locked inspection/termination points d) Alternative feeds or routing e) Avoidance of routes through public areas 	M	P
HST03.08	<p>The vendor MUST ensure that the power supply to highly sensitive facilities is protected. Methods of protection may include:</p> <ul style="list-style-type: none"> a) Using uninterruptible power supply (UPS) devices that have enough battery capacity to support the orderly shutdown of sensitive information systems b) Installing surge protection equipment c) Providing backup electricity generators in the event of an extended power supply d) Installing emergency lighting in case of main power failure e) Locating emergency power-off switches near emergency exits to facilitate rapid power-down in case of an emergency 	M	P
HST03.09	The vendor MUST ensure that their information systems are deployed in locations that meet the vendor-specified requirements for cooling, heating, humidity and air quality.	M	P
HST03.10	The vendor MUST ensure that telecommunications cabling that transmits information that supports the hosted EMR Offering is protected from interception or damage. Methods of protection may include:	M	P

OMD #	REQUIREMENT	M/O	STATUS
	<ul style="list-style-type: none"> 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. 		
HST03.11	The vendor MUST ensure that telecommunications equipment is connected to the utility provider by at least two diverse routes to prevent connection failures.	M	P
HST03.12	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).	M	P
HST03.13	<p>The vendor MUST minimize the impact of hazards in highly sensitive facilities by:</p> <ul style="list-style-type: none"> a) Locating fire extinguishers so that minor incidents can be tackled without delay b) Training agents, and where appropriate electronic service providers, in the use of fire extinguishers, other emergency/safety equipment, and emergency evacuation procedures c) Monitoring and controlling the temperature and humidity 	M	P
HST03.14	The vendor MUST ensure that fire alarms in highly sensitive facilities are monitored continuously, tested regularly and serviced in accordance with manufacturer specifications.	M	P
HST03.15	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.	M	P
HST03.16	<p>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, receiving, etc.).</p> <p>Each area MUST be assigned a physical security zone to determine the physical security controls. Physical security zones</p>	M	P

OMD #	REQUIREMENT	M/O	STATUS
	with the corresponding minimum physical security controls for the hosted EMR Offering are found in Appendix B: Physical Security Zones.		
HST03.17	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), then the maximum number of zones that may be skipped in the design of a data centre environment MUST be limited to one. In such cases, the relevant TRA MUST reflect the skipped zone, and compensating controls MUST be investigated and implemented.	M	P
HST03.18	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.	M	P
HST03.19	The vendor MUST require all agents and electronic service providers to obtain written approval from one of the vendor's senior-level executives 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.	M	P

4.3 Acceptable Use of Information and Information Technology

OMD #	REQUIREMENT	M/O	STATUS
HST04.01	The vendor, including its staff, agents, suppliers and electronic service providers ("All Persons") MUST always use their assigned ID and password to access the hosted EMR Offering.	M	P
HST04.02	All Persons MUST never allow another person to use their ID to access the hosted EMR Offering. All Persons are accountable for any actions performed with their ID on the hosted EMR Offering.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST04.03	All Persons MUST never access the hosted EMR Offering unless their role requires them to do so, they are expressly authorized to do so, it is necessary to do so (e.g., providing or assisting in the provision of health care), and in accordance with the hosted EMR Offering's privacy policies.	M	P
HST04.04	<p>All Persons MUST immediately report suspected or confirmed information security incidents to the hosted EMR Offering information security incident initial point of contact (e.g., a help desk). Alternatively, agents may report the incident to their manager or supervisor, who in turn, MUST report it to the information security incident's initial point of contact. Examples of information security incidents include, but are not limited to:</p> <ul style="list-style-type: none"> 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 Offering d) Attempts (either failed or successful) to gain unauthorized access to the hosted EMR Offering <p>Compromised password, i.e., another individual knows your password</p>	M	P
HST04.05	All Persons MUST provide their full cooperation to the vendor, their agents or electronic service providers with any information security incident investigation.	M	P
HST04.06	All Persons 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.	M	P
HST04.07	All Persons MUST never knowingly perform an act that will interfere with the normal operations of the hosted EMR Offering or try to disrupt the hosted EMR Offering by either intentionally making such services unavailable or by affecting the integrity of the data being stored in or processed by the hosted EMR Offering.	M	P
HST04.08	All Persons MUST abide by the terms and conditions of the hosted EMR Offering provided.	M	P
HST04.09	All Persons MUST never discuss PHI with any person who does not have a need-to-know or is not authorized to know the information.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST04.10	All Persons 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.	M	P
HST04.11	All Persons MUST lock up PHI in any form (e.g., locking paper, printed copies originating from the hosted EMR Offering or portable storage media in a cabinet) when left unattended in an unsecured area, especially when the office or area is vacated.	M	P
HST04.12	All Persons MUST always log off or lock unattended computers or workstations to prevent unauthorized individuals from accessing PHI.	M	P
HST04.13	All Persons MUST only store PHI on the hosted EMR Offering-approved devices or storage networks and only store the minimal amount of PHI necessary on any encrypted portable storage media.	M	P
HST04.14	All Persons MUST always ensure that paper documents containing PHI are shredded or placed in a secure shredding receptacle when they are no longer needed.	M	P
HST04.15	All Persons MUST follow internal procedures for the proper secure disposal of any information technology that may have PHI stored on it.	M	P
HST04.16	All Persons MUST only email PHI when it is necessary for providing or assisting in the provision of health care or the hosted EMR Offering business and is acceptable under the hosted EMR Offering's policies or procedures.	M	P
HST04.17	All Persons MUST encrypt all emails that contain PHI, use a secure file transfer solution or use a secure email system approved by the hosted EMR Offering.	M	P
HST04.18	All Persons MUST never use external email accounts (e.g., Hotmail, or Gmail) to send or receive PHI.	M	P
HST04.19	All Persons MUST always create a password used to access the hosted EMR Offering that is at least eight characters long and that includes at least three of the following: a) One number b) One uppercase letter c) One lowercase letter, or	M	P

OMD #	REQUIREMENT	M/O	STATUS
	d) One special character		
HST04.20	All Persons MUST never create passwords that include: a) All or part of their ID b) Easily obtained personal information about themselves (e.g., names of family members, pets, birthdays, anniversaries, hobbies) c) Three consecutive characters (e.g., AAA)	M	P
HST04.21	All Persons MUST choose passwords that are easy to remember but hard to guess by someone else.	M	P
HST04.22	All Persons MUST never change passwords in an easily recognized pattern (e.g., changing “lLOv3EatingP!zza1” to “lLOv3EatingP!zza2”).	M	P
HST04.23	All Persons MUST ensure that their passwords used to access the hosted EMR Offering are different from their password(s) used to access other accounts (e.g., corporate e-mail account, personal banking, etc.).	M	P
HST04.24	All Persons MUST commit their passwords to memory. All Persons MUST avoid keeping a record of their passwords (e.g., on paper, or stored in a file) unless it: a) Can be stored securely b) Does not indicate the ID, information system or information technology for which the ID is associated	M	P
HST04.25	All Persons MUST keep their passwords a secret, never telling anyone their password, including a system administrator, help desk personnel or a manager.	M	P
HST04.26	All Persons MUST change their password immediately if they suspect or confirm that their password has been disclosed or compromised.	M	P
HST04.27	All Persons MUST not include their ID or password in any automated sign-on process (e.g., stored in a macro or function key).	M	P
HST04.28	All Persons MUST always change passwords that are provided to them at initial login.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST04.29	All Persons MUST use the hosted EMR Offering approved remote access solution (e.g., through a virtual private network or terminal services) to remotely access the hosted EMR Offering.	M	P
HST04.30	All Persons 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).	M	P
HST04.31	All Persons MUST never access the hosted EMR Offering in an area where unauthorized individuals can view the information (e.g., Internet cafés, public transit, and other non-private settings).	M	P
HST04.32	All Persons MUST never leave their mobile computing device that has the ability to access the hosted EMR Offering unattended in a public place.	M	P
HST04.33	All Persons MUST, when required to 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.	M	P

4.4 Access to Control and Identity Management for System-Level Access

OMD #	REQUIREMENT	M/O	STATUS
HST05.01	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.	M	P
HST05.02	<p>The vendor MUST implement a process to verify job application information for all its employees, new employees, agents or electronic service providers who will have access to the hosted EMR Offering. Verification methods may include:</p> <ul style="list-style-type: none"> a) Character or employment references b) Criminal record checks where possible taking into consideration the employment arrangements of the organization and unions c) Verification of prior experience, academic record, and professional qualifications 	M	P

OMD #	REQUIREMENT	M/O	STATUS
	Verification of identity from government-issued identification		
HST05.03	<p>The vendor MUST ensure that all its new employees, agents and electronic service providers who will have access to the hosted EMR Offering agree to maintain the security of information, information systems and information technologies. At a minimum, the terms and conditions of employment MUST:</p> <ul style="list-style-type: none"> a) Require adherence to the vendor's information security-related policies b) Explain the employee, agent or electronic service provider's legal responsibilities and rights, e.g., regarding the protection of information or privacy legislation c) Include a non-disclosure/confidentiality clause that extends after employment d) State that information security responsibilities extend outside normal working hours, premises and networks, and continue after employment has ended 	M	P
HST05.04	<p>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).</p> <p>The vendor is responsible for identifying all their agents and electronic service providers who require access to the hosted EMR Offering.</p>	M	P
HST05.05	<p>The vendor MUST implement access control systems on the hosted EMR Offering. The access control system MUST have authentication and authorization capabilities that:</p> <ul style="list-style-type: none"> a) Identify and authenticate individual persons or information systems b) Limit or restrict access to an information system's resources, objects, data, and/or files 	M	P
HST05.06	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 Offering.	M	P
HST05.07	The vendor MUST ensure that access to and use of the hosted EMR Offering with a user ID is traceable to a single person and that access to and use of the hosted EMR Offering with a Service ID is traceable to an information system.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST05.08	The vendor MUST configure its access control and identity management system to deny access by default to the hosted EMR Offering (i.e., access MUST be explicitly authorized).	M	P
HST05.09	<p>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:</p> <ul style="list-style-type: none"> 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 c) Justification for the request (if applicable, e.g., when requesting a Privileged ID) 	M	P
HST05.10	The vendor MUST maintain a log of all requests for IDs that it manages and that could be used to access the hosted EMR Offering.	M	P
HST05.11	<p>The vendor MUST maintain a list of all IDs that have access to the hosted EMR Offering. The list should include the following:</p> <ul style="list-style-type: none"> a) The 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) Interactions (for Service IDs only) 	M	P
HST05.12	The vendor MUST review a list of IDs and authorizations it manages and that have access to the hosted EMR Offering annually to ensure that authorized access remains appropriate and MUST request modifications, suspensions, or revocations to privileges where inappropriate access is identified.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST05.13	Upon termination of employment, contractual or other relationship, or a change in job duties or responsibilities, the vendor MUST review and if necessary request a modification, suspension or revocation of access privileges for their employees, agents or electronic service provider.	M	P
HST05.14	The vendor MUST suspend user IDs that it manages and that have access to the hosted EMR Offering after 180 consecutive days of inactivity either manually or automatically. The vendor MAY notify the user of the ID warning them of the imminent suspension.	M	P
HST05.15	The vendor MUST not name Privileged IDs in a way that identifies or provides an indication of the IDs' privilege level (e.g., naming a service account using random characters, rather than "superuser").	M	U
HST05.16	The vendor MUST not assign privileged entitlements on their information systems or information technologies to a Personal ID. All Persons requiring privileged access MUST be assigned a Privileged ID, and a Personal ID to be used for normal business activities.	M	P
HST05.17	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.	M	P
HST05.18	The vendor MUST ensure that the names of their Service IDs used to identify their EMR Offerings are not dependent on the information system names on which the Service IDs are created.	M	P
HST05.19	The vendor MUST ensure that Service IDs are not capable of interactive sign-on.	M	P
HST05.20	The vendor MUST ensure that an identified owner is assigned to each Service ID.	M	P
HST05.21	The vendor MUST use a non-expiring password for Service IDs with credentials that are incapable of being used by a person.	M	P
HST05.22	The vendor MUST ensure that a Service ID with credentials that are capable of being used by a person and are embedded into an automated process to change to a new password either: <ul style="list-style-type: none"> a) Whenever the technology changes b) After an actual or suspected password compromise, or 	M	P

OMD #	REQUIREMENT	M/O	STATUS
	c) After the departure of any person who knows the password		
HST05.23	The vendor MUST ensure that authentication methods that employ the criteria of “something you have” (e.g., digital certificate, SecureID token) permit the unique identification of each person and are not used concurrently by multiple EMR users.	M	P
HST05.24	The vendor MUST communicate initial passwords or passphrases (“passwords”) securely. Where an ID has been communicated through email, the associated password MUST be communicated through an alternative communication channel (e.g., via phone).	M	P
HST05.25	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.	M	P
HST05.26	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.	M	P
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 C: Minimum Password Requirements for more information.	M	P
HST05.28	The vendor MUST only reset a password after the EMR user’s identity has been successfully verified.	M	P
HST05.29	The EMR Offering MUST encrypt passwords in transmission.	M	P
HST05.30	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.	M	P
HST05.31	The vendor MUST not cache unencrypted passwords.	M	P
HST05.32	The vendor MUST not hard-code clear text passwords in information systems or stored in batch files or scripts.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST05.33	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.	M	P
HST05.34	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.	M	P
HST05.35	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.	M	P
HST05.36	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).	M	P
HST05.37	The vendor MUST rename all default IDs (commonly known as vendor IDs).	M	P
HST05.38	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.	M	P
HST05.39	The vendor MUST ensure that additional authentication compensating factors (e.g., two-factor authentication or through the use of challenge questions) are required to access the hosted EMR Offering remotely or from an untrusted source.	M	P
HST05.40	The vendor MUST ensure that remote access for any of their EMR users who have privileged access to the hosted EMR Offering, directly or indirectly (e.g., through the escalation of privileges), is permitted only through the use of the hosted EMR Offering-approved virtual workspace computing solution.	M	P
HST05.41	<p>The vendor MUST maintain a record of all their staff, agents and electronic service providers that have authorized administrative remote access to the hosted EMR Offering. At a minimum, the record MUST contain:</p> <ul style="list-style-type: none"> a) The agent or electronic service provider's user ID b) The agent or electronic service provider's full name c) The date of creation d) The level of entitlement granted 	M	P

OMD #	REQUIREMENT	M/O	STATUS
	e) The full name and position of the person who authorized the request		
HST05.42	The vendor MUST employ cryptographic solutions to maintain session confidentiality and integrity of all remote access connections.	M	P
HST05.43	The vendor MUST ensure that Privileged IDs are not capable of establishing multiple concurrent interactive sessions to the hosted EMR Offering.	M	P
HST05.44	The vendor MUST ensure that the state of a session is established and controlled by the information system providing the services.	M	P
HST05.45	The vendor MUST implement session management mechanisms to protect session integrity and confidentiality (e.g., using Kerberos to maintain session integrity and using encryption to provide session confidentiality).	M	P
HST05.46	The vendor MUST ensure that session management identifiers are unique for each individual session and are valid only for the duration of the current session or for a pre-determined finite period.	M	P
HST05.47	The vendor MUST ensure that all EMR users have the ability to end or terminate an active session.	M	P
HST05.48	The vendor MUST ensure that an interruption to a communication link to the source information system requires the person or information system to re-authenticate to the source information system.	M	P
HST05.49	<p>The vendor MUST ensure that workstations and other EMR user devices that have access to the hosted EMR Offering either:</p> <ul style="list-style-type: none"> a) Have password-protected screen-locks, keyboard-locks or equivalent controls that are set to automatically lock after 15 minutes of inactivity, or b) Set sessions to automatically terminate (e.g., sign-off active account) after a maximum period of 15 minutes of inactivity 	M	P

4.5 Information and Asset Management

OMD #	REQUIREMENT	M/O	STATUS
HST06.01	The vendor MUST implement and maintain an information and asset classification scheme for the confidentiality, availability and integrity of all information and assets it owns or manages. See Appendix D: Information Asset Management for more information.	M	P
HST06.02	The vendor MUST label information and assets in accordance with the labelling requirements listed in Appendix D: Information Asset Management	M	P
HST06.03	The vendor MUST ensure that all PHI and all assets that process or store PHI are protected, at a minimum, in accordance with Appendix D: Information Asset Management Requirements. The vendor may choose to implement additional controls than those required in Appendix D: Information Asset Management	M	P
HST06.04	When information is combined or aggregated with information of a lower classification, the vendor MUST ensure that the highest classification level contained therein shall determine, at a minimum, the overall classification of all the information.	M	P
HST06.05	The vendor MUST ensure that all copies of paper material that is classified as restricted be individually numbered at the time of creation and that a master list associating each numbered copy to whom the individual that it was distributed is maintained.	M	P
HST06.06	The vendor MUST encrypt all information (PHI and the hosted EMR Offering Data) classified as Internal or higher from integrated storage devices and removable media prior to being sent externally. The removal of information classified as Confidential or higher MUST be done in a manner such that the information cannot be recovered and viewed by unauthorized individuals.	M	U
HST06.07	The vendor MUST log the destruction of the PHI in the hosted EMR Offering database, as soon as possible, but no later than five days after the destruction. At a minimum, the log MUST include the:	M	P

OMD #	REQUIREMENT	M/O	STATUS
	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 d) Identity of the person who destroyed the PHI e) Identity of the person who authorized the destruction of the PHI		

4.6 Information Security Incident Management

OMD #	REQUIREMENT	M/O	STATUS
HST07.01	The vendor MUST implement an information security incident ("incident") management process that covers all phases of the incident management process: a) Identification/Triage b) Response c) Recovery d) Follow-up	M	P
HST07.02	If at any point in the incident management process, the vendor realizes that the incident has resulted in a privacy breach, then the incident MUST be handled in accordance with the vendor's Privacy Breach Management Policy.	M	P
HST07.03	The vendor MUST establish a point of contact to which actual or suspected incidents are reported. Most often, the point of contact is a service desk.	M	P
HST07.04	The vendor MUST ensure that all its staff, agents and electronic service providers are aware of their responsibility to immediately report actual or suspected incidents.	M	P
HST07.05	The point of contact MUST generate an incident ticket for all reported incidents. An automated incident management system is recommended to support the recording of incidents. The incident ticket MUST contain the following elements: a) The time and date of the reported incident	M	P

OMD #	REQUIREMENT	M/O	STATUS
	b) The name and contact information of the subscriber, EMR user, agent or electronic service provider that reported the incident c) Details about the reported incident, (e.g., type and how it was detected) d) Any impacts of the reported incident e) Any actions undertaken to contain the incident either by the agent or electronic service provider that reported the incident or the point of contact		
HST07.06	The vendor MUST appoint an incident response lead or team who is responsible for initiating the triage, response, recovery and follow-up activities for all incidents. The incident response lead or team may be the same as the point of contact.	M	P
HST07.07	The point of contact MUST immediately send all incident tickets to the incident response lead or team.	M	P
HST07.08	The incident response lead or team MUST review the incident ticket and any supporting information to verify whether or not an incident has occurred.	M	P
HST07.09	The incident response lead or team MUST classify all actual incidents according to severity. Please see Appendix E: Information Security Incident Management for more information.	M	P
HST07.10	The incident response lead or team MUST initiate an incident report. Please see Part Two, Appendix E: Information Security Incident Management for more information.	M	P
HST07.11	All completed or partially completed incident reports MUST be handled, at a minimum, in accordance with the protection requirements for information classified as Confidential. Please see Part Two, Appendix E: Information Security Incident Management for more information.	M	P
HST07.12	If an incident that originates at a HIC affects multiple HICs or the hosted EMR Offering, the vendor MUST assume leadership of the incident management activities.	M	P
HST07.13	The vendor MUST ensure that their incident management process requires the incident response lead or team to notify any affected subscribers by email by the end of the next business day of any incident that the vendor classifies as a Severity 1 (Critical) or Severity 2 (High).	M	P

OMD #	REQUIREMENT	M/O	STATUS
	<p>At a minimum, the notification MUST contain the following elements:</p> <ul style="list-style-type: none"> a) The time and date of the reported incident b) The name and contact information of the agent or electronic service provider that reported the incident c) Details about the reported incident (e.g., type and how it was detected) d) Any impacts of the reported incident e) Any actions undertaken to contain the incident either by the agent or electronic service provider that reported the incident, the point of contact, or the incident response lead or team 		
HST07.14	<p>The vendor MUST notify OMD:</p> <ul style="list-style-type: none"> a) Within 48 hours of the incident for any incident classified as a Severity 1 (Critical) b) Within one week of the incident for any incident classified as a Severity 2 (High) 	M	P
HST07.15	<p>The vendor MUST prioritize all incidents in accordance with their severity and priority rating.</p>	M	P
HST07.16	<p>The incident response lead or team MUST take steps to limit the scope and magnitude of an incident. Mitigation or containment activities may include:</p> <ul style="list-style-type: none"> a) Backing up the information system b) Discontinuing operations c) Changing passwords or modifying access control lists on the compromised information system d) Restricting connectivity <p>Note: Depending on the severity of an incident it may be necessary to activate the vendor's business continuity plans.</p>	M	P
HST07.17	<p>The vendor MUST remediate all applicable information systems so that they return to full and normal operations. Remediation activities may include:</p> <ul style="list-style-type: none"> a) Eradicating the cause of the incident (e.g., removing malware) b) Restoring and validating the information system c) Deciding when to restore operations 	M	P

OMD #	REQUIREMENT	M/O	STATUS
	d) Monitoring information systems to verify normal operations without further information system or data compromise		
HST07.18	The vendor MUST investigate all incidents to identify the cause of the incident (e.g., by performing root cause analysis.)	M	P
HST07.19	Once an incident has been resolved (i.e., all remediation activities have been implemented and affected information systems and information technology have returned to full and normal operations), the incident response lead or team MUST complete the incident report. During longer investigations, affected subscribers may request status updates on the incident investigation in the interim.	M	P
HST07.20	The vendor MUST archive their incident reports for a minimum of 24 months.	M	P
HST07.21	The vendor MUST provide OMD with incident reports upon request, within 72 hours of the request.	M	P
HST07.22	The vendor MUST implement a mechanism to review all of their incidents, at a minimum, monthly, to identify trends and to determine whether any preventative actions can be taken to reduce the likelihood of similar incidents occurring in the future.	M	P
HST07.23	<p>The vendor MUST develop procedures for collecting evidence for disciplinary or legal action against agents or electronic service providers. These procedures MUST require:</p> <ul style="list-style-type: none"> a) forensics work to be performed on copies of the evidential material b) the creation of copies is witnessed <p>Details of the creation MUST be logged, including:</p> <ul style="list-style-type: none"> a) when and where the copying process was executed b) who performed the copying activities c) which tools or programs were utilized for the copying process d) how the integrity of all evidential material is protected 	M	P

4.7 Business Continuity

OMD #	REQUIREMENT	M/O	STATUS
HST08.01	<p>The vendor MUST ensure that information security and information technology requirements are embedded in their business continuity strategy, and address the following:</p> <ul style="list-style-type: none"> 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 	M	P
HST08.02	<p>The vendor MUST ensure that the business continuity strategy identifies the information systems to be supported by business continuity plans and arrangements, and records relevant details (e.g., in a business continuity risk register) about:</p> <ul style="list-style-type: none"> a) Critical information systems (ranked in order of priority) and the business processes they support b) Key internal and external stakeholders 	M	P
HST08.03	<p>The vendor MUST ensure that the hosted EMR Offering is robust, reliable and supported by alternate or duplicate facilities.</p>	M	P
HST08.04	<p>The vendor MUST implement methods to reduce the likelihood of critical information systems malfunctioning, which MUST include:</p> <ul style="list-style-type: none"> a) Employing up-to-date makes/models of hardware and software that are easily maintained and can meet the requirements of critical business processes b) Giving high priority to reliability, compatibility and capacity during the acquisition process c) Ensuring compliance with common or industry security standards for hardware and software d) Using telecommunication network links and services that are robust and resilient 	M	P
HST08.05	<p>The vendor MUST implement methods to ensure that the availability of critical information systems is maintained, which may include:</p> <ul style="list-style-type: none"> a) Running the critical information systems simultaneously at multiple locations (e.g., by using hot stand-by or virtualization) b) Providing alternative locations from which information systems can be run and administered 	M	P

OMD #	REQUIREMENT	M/O	STATUS
	c) Automatically identifying and recovering transactions following an information system failure		
HST08.06	<p>The vendor MUST reduce single points of failure in their network, which may include:</p> <ul style="list-style-type: none"> a) Rerouting network traffic automatically when critical network equipment or links fail 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 	M	P
HST08.07	<p>The vendor MUST develop a method for dealing with faults, which may include:</p> <ul style="list-style-type: none"> 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	P
HST08.08	The vendor MUST ensure that a business continuity plan is created for each information system (or group of related information systems) as part of the wider business continuity strategy.	M	P
HST08.09	The vendor MUST appoint an owner for each information system (or group of related information systems) who is responsible for developing, testing, and executing business continuity plans and arrangements for their information systems.	M	P
HST08.10	<p>The vendor MUST base the business continuity plan on the results of a risk assessment, which MUST include:</p> <ul style="list-style-type: none"> 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 c) 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	P
HST08.11	The business continuity plan for each critical information system (or group of related critical information systems) MUST include:	M	P

OMD #	REQUIREMENT	M/O	STATUS
	<ul style="list-style-type: none"> 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) 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) h) Ownership of the specific plan and a record of the most recent review for the adequacy of the plan i) Necessary stakeholder and responsible party contact information and communications plan 		
HST08.12	<p>At a minimum, the vendor MUST review and test their business continuity plans annually, which MUST include at least one of the following, with each scenario being tested within a period of three years:</p> <ul style="list-style-type: none"> 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, or c) Complex tests, which involve full-interruption tests where the original site is shut down and a complete test is performed at an alternative facility 	M	P
HST08.13	<p>The vendor MUST maintain a record of the execution of the tests with the date, the results, and sign-off from a senior-level executive (e.g., CIO).</p>	M	P

4.8 Cryptography

OMD #	REQUIREMENT	M/O	STATUS
HST09.01	Only the hosted EMR Offering-approved cryptographic algorithms shall be implemented on the hosted EMR Offering. A list of approved cryptographic algorithms can be found in Appendix F: Approved Cryptographic Algorithms.	M	P
HST09.02	The vendor MUST ensure that each proposed implementation of a cryptographic solution on the hosted EMR Offering is assessed by an information security specialist.	M	P
HST09.03	The vendor MUST only implement cryptographic solutions that fail close (i.e., access is denied if a failure occurs).	M	P
HST09.04	The vendor MUST ensure that all implementations of cryptography have documented contingency procedures prior to production implementation. These procedures MUST be made available to all relevant stakeholders.	M	P
HST09.05	The vendor MUST use hardware cryptography (rather than software cryptography) in environments that store or process PHI.	M	P
HST09.06	Where cryptographic hardware devices are used, the 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.	M	P
HST09.07	The vendor MUST only permit software cryptography solutions to only be permitted for: <ul style="list-style-type: none"> a) One-way (or non-reversible) cryptographic functions b) Client-side software for remote access c) Client-side storage encryption such as full-disk encryption d) Client-side or server-side digital certificates, or e) Data storage in data centres. 	M	P
HST09.08	Where software-based cryptography is implemented, the vendor MUST ensure that the password is not stored in a program, batch file, or script file, with the exception of server-based SSL digital certificates, which MUST have strict access control placed on the file that contains the password.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST09.09	The vendor MUST cryptographically protect the integrity of its cryptographic keys, especially when its cryptographic keys are located in a publicly accessible location (e.g., Internet-facing web server).	M	P
HST09.10	The vendor MUST ensure that MAC values are appended to the data from which it is calculated.	M	P
HST09.11	The vendor MUST ensure that all hash functions are one-way (i.e., non-reversible).	M	P
HST09.12	The vendor MUST only use a digital signature for the purpose of signing.	M	P
HST09.13	The vendor MUST ensure that all digital certificates are revocable.	M	P
HST09.14	The vendor MUST implement digital certificates with a cryptographically secured certificate revocation list (CRL) system.	M	P
HST09.15	The vendor MUST ensure that a digital certificate is only trusted once it has been cryptographically validated and does not appear on a trusted CRL.	M	P
HST09.16	The vendor MUST protect its cryptographic keys against unauthorized access (in the case of secret and private keys), modification, loss, and accidental or intentional destruction.	M	P
HST09.17	The vendor MUST ensure that equipment used to generate, load, store and archive cryptographic keys is physically protected against unauthorized access or modification.	M	P
HST09.18	<p>The vendor MUST establish a process for managing cryptographic keys, which covers:</p> <ul style="list-style-type: none"> a) The secure generation, distribution, loading, storage, recovery, replacement, revocation and destruction of cryptographic keys b) The secure backup and archive of cryptographic keys <p>These processes and procedures MUST be made available to all relevant stakeholders.</p>	M	P
HST09.19	The vendor MUST maintain an inventory for all their cryptographic keys and key components. The inventory should include the following:	M	P

OMD #	REQUIREMENT	M/O	STATUS
	a) Key name and purpose/usage b) Key type c) Key generation date d) Component number, including the total number of components e) Storage location(s) f) All key custodians since generation, including the dates of custodial changes g) The date the key was destroyed, and proof of destruction		
HST09.20	The vendor MUST review the inventory of its cryptographic keys annually.	M	P
HST09.21	The vendor MUST maintain logs to record any instance in which keys, key components, or related materials are generated, removed from storage or loaded to a cryptographic device. The logs should include: a) Key name and purpose/usage b) Date and time c) Component identifier d) Purpose of access e) Name and signature of custodian accessing the component f) Tamper-evident package number prior to removal (if applicable)	M	P
HST09.22	The vendor MUST review the audit logs of its keys annually.	M	P
HST09.23	The 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	P
HST09.24	The vendor MUST store keys in the fewest possible locations and forms.	M	P
HST09.25	The vendor MUST ensure that backup copies of secret keys exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups MUST exist only in one of the allowed storage forms for that key.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST09.26	The 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.	M	P
HST09.27	The 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.	M	P
HST09.28	The vendor MUST ensure that secret keys and key components that are no longer used or have been replaced are securely revoked and destroyed.	M	P
HST09.29	The vendor MUST only permit a key generation process to be initiated by the key custodian.	M	P
HST09.30	The 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 as defined in the NIST Special Publication (SP) 800-22 Revision 1a.	M	P
HST09.31	To ensure the confidentiality of their secret keys, the vendor MUST ensure that a secret key only exists in the following forms: a) As clear text inside the protected memory of a tamper-resistant security module (TRSM) b) As cypher text outside the protected memory of a TRSM, or c) As two or more components, held under split knowledge and dual control	M	P
HST09.32	The vendor MUST ensure that the output of the key generation process is monitored by at least two authorized agents or electronic service providers.	M	P
HST09.33	The 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.	M	P
HST09.34	The 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.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST09.35	The 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.	M	P
HST09.36	The 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.	M	P
HST09.37	The 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.	M	P
HST09.38	The vendor MUST ensure that unencrypted secret keys are entered into cryptographic devices using the principles of dual control and split knowledge. In instances where a secure key-loading device is used, only dual control is required.	M	P
HST09.39	The vendor MUST ensure that any hardware used in the key-loading function is controlled and maintained in a secure environment under dual control.	M	P
HST09.40	The 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.	M	P
HST09.41	The vendor MUST define and implement procedures to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key or key component for another, or the operation of any cryptographic device without legitimate keys or key components.	M	P
HST09.42	The 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.	M	P
HST09.43	The vendor MUST ensure that all secret keys used for any function are unique (except by chance) to that device.	M	P
HST09.44	A certificate key lifespan MUST be no longer than seven years.	M	P
HST09.45	The vendor MUST ensure that an uncompromised key is replaced on or before its stipulated lifespan.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST09.46	<p>If a key or key component has been compromised or is suspected of being compromised, the vendor MUST:</p> <ul style="list-style-type: none"> a) Replace the compromised or suspected compromised key as soon as possible. The replacement key MUST not be a variant of the original key b) Inspect the cryptographic device for any form of unauthorized modification before installing the new key or key component 	M	P
HST09.47	The 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.	M	P
HST09.48	<p>The vendor MUST ensure that the destruction of a key is witnessed by the key custodians with the appropriate records retained for audit purposes. Each key or key component destruction should record the following:</p> <ul style="list-style-type: none"> a) The date and time of the keying material destruction b) The reason for destroying the keying material c) The full name and signature of the individual authorizing the destruction d) The full name and signature of the individual destroying the keying material e) The full name and signature of the persons witnessing the destruction 	M	P
HST09.49	The Chief Information Officer or their delegate MUST assign the key custodian(s) responsible for each key.	M	P
HST09.50	The vendor MUST ensure that key custodians handle the key or key component in their custody in a Restricted manner as described in Section B, Requirement 5.0 Information Asset Management.	M	P
HST09.51	The vendor MUST ensure that key custodians assigned to cryptographic keys are limited to the fewest number of key custodians necessary.	M	P
HST09.52	The 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.	M	P
HST09.53	The 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.	M	P

4.9 Security Logging and Monitoring

OMD #	REQUIREMENT	M/O	STATUS
HST10.01	The vendor MUST enable logging by default on the hosted EMR Offering.	M	P
HST10.02	The vendor MUST ensure that their logging capabilities are enabled and operational at all times. The vendor MUST configure their information systems in a manner such that they are disabled if logging is not operational.	M	P
HST10.03	The vendor MUST ensure that all logs are classified in accordance with the highest level of information contained within the logs.	M	P
HST10.04	The vendor MUST log all information system events/activities found in Appendix G: Security Logging and Monitoring – performed by an EMR user, agent, and electronic service provider.	M	P
HST10.05	The vendor MUST log all activities of their information system administrators and information system operators as part of the general audit trail process.	M	P
HST10.06	<p>The vendor MUST ensure that all logs, at a minimum and where relevant, contain the following information for each event/activity:</p> <ul style="list-style-type: none"> a) Identifiers (as many as available) for the subject requesting the action (e.g., EMR user ID, computer name, IP address, and MAC address) b) Identifiers (as many as available) for the object the action was performed on (e.g., file names accessed, unique identifiers of records accessed in a database, IP address, and MAC address) c) Date and time d) The event activity (e.g., sign-on and sign-off) e) Status of the security event activity (e.g., success or failure, denied or allowed) f) Type of access (e.g., read, write, execute) g) Alarms raised by access control and network monitoring systems 	M	P
HST10.07	The vendor MUST not filter logs at the source.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST10.08	The vendor MUST synchronize their information system clocks to a centralized clock source. The vendor MUST perform clock synchronization validation, at a minimum, daily to ensure ongoing clock synchronization accuracy.	M	P
HST10.09	The vendor MUST implement controls to protect the confidentiality and integrity of logs both in storage and during transmission.	M	P
HST10.10	The vendor MUST restrict all access to logs based on the principles of least privilege and need-to-know.	M	P
HST10.11	<p>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:</p> <ul style="list-style-type: none"> 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 e) Name/type of log to which the agent or electronic service provider has access 	M	P
HST10.12	The vendor MUST not configure logs to overwrite old data when the maximum log size limit has been reached.	M	P
HST10.13	The vendor MUST prohibit their agents and electronic service providers with authorized access to logs from erasing or deactivating logs of their own activities.	M	P
HST10.14	The vendor MUST ensure that the management of log generation sources is logged and controlled via documented change control procedures.	M	P
HST10.15	The vendor MUST implement automated mechanisms on their information systems to consolidate logs to centralized log management servers.	M	P
HST10.16	The vendor MUST implement automated tools on their information systems to convert logs with different content and formats to a single standard format with consistent data field representations.	M	P
HST10.17	The vendor MUST monitor their logs to ensure that:	M	P

OMD #	REQUIREMENT	M/O	STATUS
	a) Log triggers are appropriately configured b) Log triggers are not compromised c) Faults are identified for further analysis and remediation steps d) Identified faults are resolved or mitigated		
HST10.18	The vendor MUST implement automated analysis tools on their information systems to assist in the detection and prevention of information and information system misuse or intrusion.	M	P
HST10.19	The vendor MUST implement automated correlation tools on their information systems to look for patterns of events/activities across multiple information systems.	M	P
HST10.20	The vendor MUST ensure that automated alerts are triggered for unsuccessful authentication attempts.	M	P
HST10.21	The vendor MUST review their logs, at a minimum, monthly to detect anomalous events on the network or the hosted EMR Offering agent or electronic service provider behaviour that is outside of policy or procedures, or to identify automated alerts generated that may indicate attacks or break-ins.	M	P
HST10.22	The vendor MUST ensure that information system administrator and operator logs are reviewed, at a minimum, monthly.	M	P
HST10.23	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 he/she manages.	M	P
HST10.24	The vendor MUST ensure that their logs relating to production data are readily available online, at a minimum, for six months.	M	P
HST10.25	The vendor MUST retain archived information system logs for a minimum duration as set out in the Ontario Health (Digital Services) CPC Data Retention Policy.	M	P
HST10.26	The vendor MUST retain archived logs of HIC, agent, and electronic service provider activities in accordance with the Ontario Health (Digital Services) CPC Data Retention Policy.	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST10.27	The vendor MUST ensure that logs related to backups are readily available online for the same period as logs related to production data.	M	P
HST10.28	The vendor MUST archive their logs in a format that can be restored for as long as data retention is required.	M	P
HST10.29	The vendor MUST label and store their archive logs in an organized manner for easy retrieval.	M	P
HST10.30	Upon retention expiry, the vendor MUST ensure that their logs are disposed of in accordance with the requirements defined in Part One, Section B, Requirement 5.0 Information Asset Management.	M	P

4.10 Electronic Service Provider

OMD #	REQUIREMENT	M/O	STATUS
HST11.01	The vendor MUST identify electronic service providers and categorize them according to supplier type (e.g., application service provider, network service provider, storage service provider, etc.) and the criticality of the services they provide.	M	P
HST11.02	<p>The vendor MUST maintain formal documentation of the:</p> <ul style="list-style-type: none"> a) Technical and organizational relationships covering the roles and responsibilities under the Personal Health Information Protection Act (PHIPA) and its regulations and under the privacy and information security policies and procedures that electronic service providers are required to fulfill b) Roles and responsibilities for implementing, maintaining and supporting the information systems or services that the electronic service providers are required to fulfill c) Electronic service provider's service goals d) Electronic service provider's expected deliverables e) Representatives of electronic service providers <p>Formal documentation may include contracts, agreements and service levels</p>	M	P

OMD #	REQUIREMENT	M/O	STATUS
HST11.03	The vendor MUST assess the potential information security and privacy risks posed by electronic service providers to the hosted EMR Offering prior to engaging in a contractual relationship with that electronic service provider.	M	P
HST11.04	<p>The vendor MUST define and document all information systems and services to be provided by any new electronic service provider or on renewal of any service agreements. At a minimum, the vendor service agreements with electronic service providers MUST specify:</p> <ul style="list-style-type: none"> a) Roles and responsibilities under PHIPA and the privacy and information security policies and procedures implemented in respect of the hosted EMR Offering b) Roles and responsibilities for implementing, maintaining and supporting the information systems or services to be provided: <ul style="list-style-type: none"> I. The level of criticality of the service II. The dates and times when the service is required III. The capacity requirements of systems and networks IV. Maximum permissible downtime and service level objectives V. Service level reports and frequency VI. Critical timescales, i.e., the timescale beyond which a loss of service would be unacceptable to the hosted EMR Offering VII. The remedies to be imposed in the event the electronic service provider fails to deliver the agreed level of service or fails to fulfill its roles and responsibilities VIII. Minimum information security and privacy controls. 	M	P
HST11.05	The 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 Offering.	M	P
HST11.06	The vendor MUST ensure that threat risk assessments are performed on their electronic service providers.	M	P
HST11.07	<p>The vendor MUST establish a consistent method for handling the termination of the electronic service provider relationship, which MUST include:</p> <ul style="list-style-type: none"> a) Designating agents responsible for managing the termination b) Revocation of physical and logical access rights to the organization's information 	M	P

OMD #	REQUIREMENT	M/O	STATUS
	c) Secure return, transfer or destruction of all assets (e.g. backup media storage, documentation, hardware, and authentication devices)		
HST11.08	<p>The vendor MUST establish contingency arrangements to ensure that their respective business processes can continue in the event that the electronic service provider is not available (e.g., due to contract termination, a disaster, or labour disputes). These arrangements should be based on the results of a threat and risk assessment which may include:</p> <ul style="list-style-type: none"> a) The provision of alternative, secure facilities for business processes to continue b) Escrow of information and close/propriety technologies (e.g., application source code and cryptographic keys using a trusted external party, such as a lawyer c) Recovery arrangements to ensure continued availability of information stored at an outsource provider or in the cloud; or d) Alignment with the hosted EMR Offering's business continuity program 	M	P

5. APPENDICES

5.1 Appendix A: Glossary

TERM	DEFINITION
All persons	The vendor, including its staff, agents, suppliers and electronic service providers.
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 Offering, with elevated privileges, that is managed by the vendor.
User ID (managed by vendor)	Credentials within the EMR Offering that are managed by the vendor.

5.2 Appendix B: Physical Security Zones

ZONES	DESCRIPTION	REQUIREMENTS
Public Zone	<p>Any public entrance to a physical facility and the immediate environment around it is considered a public zone.</p> <p>Public zone examples include:</p> <ul style="list-style-type: none"> • Facility parking lots • Grounds surrounding a facility • Any area of unimpeded public access during posted business hours. 	No special requirements for public zones, as it is not always possible to manage these environments directly.

ZONES	DESCRIPTION	REQUIREMENTS
Reception Zone	<p>A reception zone is an area where public access intersects with facility staff or operations for administrative reasons or to obtain access.</p> <p>Reception zone examples include:</p> <ul style="list-style-type: none"> • The main entrance of a facility or a floor in shared accommodation situations; • Visitor receiving and waiting areas; and • Public service desks and kiosks. 	<ul style="list-style-type: none"> • 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	<p>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.</p> <p>Operation zone examples include:</p> <ul style="list-style-type: none"> • Storage closets • Employee offices and similar areas 	<ul style="list-style-type: none"> • 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	<p>A security zone is an area within the facility that is monitored continuously and is accessible to authorized personnel and approved/escorted visitors only.</p> <p>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.</p>	<ul style="list-style-type: none"> • 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; • 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	<p>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</p>	<ul style="list-style-type: none"> • 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.

ZONES	DESCRIPTION	REQUIREMENTS
	processing environment that must be physically separated from raised floor operations is appropriate for inclusion within a high-security zone.	<ul style="list-style-type: none"> • 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).

5.3 Appendix C: Minimum Password Requirements

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

	Personal IDs & Privileged IDs	Service IDs
Length	Be at least 8 characters	Be at least 15 characters
Complexity	Contain at least three of the following: <ul style="list-style-type: none"> At least one uppercase character (A through Z) At least one lowercase character (a through z) At least one numerical digit (zero through nine) At least one non-alphanumeric character (~!@#\$%^&* _+= ' \ () { } [] ; : " < > , . ? /); 	Contain at least all of the following: <ul style="list-style-type: none"> At least one uppercase character (A through Z) At least one lowercase character (a through z) At least one numerical digit (zero through nine) At least one non-alphanumeric character (~!@#\$%^&* _+= ' \ () { } [] ; : " < > , . ? /);
Additional Password Attributes	<ul style="list-style-type: none"> Where available, software that prohibits the use of recognizable patterns must be used; Passwords must not include all or part of the EMR user's first/last names or any easily obtained personal (e.g., names of family members, pets, birthdays, anniversaries, all or part of a Login ID or a commonly known nickname). See the requirements in the section titled: Acceptable Use of Information and Information Technology. Initial or temporary passwords must be unique, not guessable, follow the password strength requirements and communicated securely following the requirements of this Policy, Passwords must not be blank and null passwords must not be used; and Guest passwords must be disabled. 	
Expiration	120 days	Service IDs are not required to be changed on a scheduled basis however equipment MUST use a new password when technologies change.
Account Lockout	After 10 unsuccessful consecutive attempts	

	Personal IDs & Privileged IDs	Service IDs
Lockout duration	Until manually unlocked by: <ul style="list-style-type: none"> • An administrator, or • A self-service password reset facility. – OR – Unlocked after a minimum of 30 minutes	
History	Last four passwords	
Minimum Age	Two days	

5.4 Appendix D: 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	<p>Information or assets that are used in the normal course of business and that is unlikely to cause harm</p> <p>Available to public</p>	<ul style="list-style-type: none"> Information found on the externally hosted EMR Offering website External job postings 	<ul style="list-style-type: none"> No impact if made publicly available If lost, would not result in injury to patients, the hosted EMR Offering 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 Offering, its agents or electronic service providers, or HICs, their agents or electronic service providers
Internal	LOW	<p>Information or assets that have a low sensitivity outside of the hosted EMR Offering and could have low levels of impact on service levels or performance, or result in low levels of financial loss</p> <p>Available to all agents of the hosted EMR Offering and electronic service providers of the hosted EMR Offering and HICs with a need-to-know</p>	<ul style="list-style-type: none"> User manuals for the hosted EMR Offering applications High-level hosted EMR Offering planning documents High-level financial information concerning the effective operation of the hosted EMR Offering 	<ul style="list-style-type: none"> Low degree of risk if made publicly available Loss of integrity or availability may have minimal adverse impact on patients, the hosted EMR Offering, 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	<p>Information or assets that have a moderate to high sensitivity within the hosted EMR Offering and outside of the hosted EMR Offering and could have a moderate impact on service levels or performance, or result in moderate levels of financial loss</p> <p>Available only to a specific function, group or role in the hosted EMR Offering, its agents or electronic service providers or HICs, their agents or electronic service providers</p>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Loss of reputation Loss of confidence in the hosted EMR Offering 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 Offering, its agents or electronic service providers, or HICs, their agents or electronic service providers
PHI	HIGH	<p>All PHI</p> <p>Available only to a specific function, group or role in the hosted EMR Offering, its agents or electronic service providers or HICs, their agents or electronic service providers</p>	PHI	<ul style="list-style-type: none"> Loss of reputation Loss of personal health information privacy Loss of confidence in the hosted EMR Offering Loss of integrity or availability may have moderate to serious adverse impact on a patient, the hosted EMR Offering, 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	<p>Information or assets that are extremely sensitive, both inside and outside of the hosted EMR Offering, could have a high impact on service levels or performance or result in high levels of financial loss</p> <p>Available only to named individuals or specified positions. (e.g., John Doe or Vice-President of Operations), in the hosted EMR Offering, its agents or electronic service providers or HICs, their agents or electronic service providers</p>	<ul style="list-style-type: none"> • Cryptographic Keys • Passwords • Hardware Security Modules 	<ul style="list-style-type: none"> • Loss of reputation • Significant financial impact • Loss of significant amounts of personal health information privacy • Loss of confidence in the hosted EMR Offering • Destruction of partnerships and relationships • Loss of integrity or availability may have a serious to extreme adverse impact on patients, the hosted EMR Offering, its agents or electronic service providers, or HICs, their agents or electronic service providers

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

5.5 Appendix E: 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	<p>Critical</p> <ul style="list-style-type: none"> 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 <p>Immediate response and restore – “all hands on deck”.</p>	30 minutes	4 hours	12 hours
2	<p>High</p> <ul style="list-style-type: none"> Single, critical site down Loss of non-mission-critical service Help desk unavailable Service degradation affecting HICs <p>Response/restore as quickly as possible - within one business day</p>	2 hours	8 hours	24 hours
3	<p>Medium</p> <ul style="list-style-type: none"> Application or physical component slow-downs Minor technical or functional problems Application or component failure affecting a single client <p>Restore within the next few business days</p>	4 hours	36 hours	48 hours

Severity	Category and Description	Recommended Maximum Time Frames		
		Triage	Containment	Recovery
4	Low <ul style="list-style-type: none"> 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)

3. General Comments
4. Summary of the Incident
5. Contact information for all involved parties
6. Log of containment/mitigation actions taken by incident response lead/team
7. List of evidence gathered
8. Cause of the Incident (e.g., misconfigured application, unpatched host)
9. List of recommended and implemented remediation activities
10. Current Status of the Incident Response

5.6 Appendix F: Approved Cryptographic Algorithms

Algorithm	Minimum Key Length	Appropriate Usage	
Symmetric Key Algorithms			
AES	128-bits	Data encryption: <ul style="list-style-type: none">• Session• Storage<ul style="list-style-type: none">○ Backup○ Archival	Key encryption: <ul style="list-style-type: none">• Session• Storage<ul style="list-style-type: none">○ Backup○ Archival
Skipjack	80-bits, with 32 iterations	Data encryption: <ul style="list-style-type: none">• Session• Storage<ul style="list-style-type: none">○ Backup○ Archival, < five years	
Triple DES	112-bits	Data encryption: <ul style="list-style-type: none">• Session• Storage<ul style="list-style-type: none">○ Backup○ Archival	Key encryption: <ul style="list-style-type: none">• Session• Storage<ul style="list-style-type: none">○ Backup○ Archival
Asymmetric Key Algorithms			

Algorithm	Minimum Key Length	Appropriate Usage	
Elliptic Curve	160-bits	Data encryption: <ul style="list-style-type: none"> • Session • Storage <ul style="list-style-type: none"> ○ Backup ○ Archival • Digital Signature 	Key encryption: <ul style="list-style-type: none"> • Session • Storage <ul style="list-style-type: none"> ○ Backup ○ Archival • Session key establishment
RSA	2048-bits	Data encryption: <ul style="list-style-type: none"> • Session • Storage <ul style="list-style-type: none"> ○ Backup ○ Archival • Digital Signature • 	Key encryption: <ul style="list-style-type: none"> • Session • Storage <ul style="list-style-type: none"> ○ Backup ○ Archival • Session key establishment
MACs and Hashes			
AES MAC	128-bits	Message authentication	
MD5 ¹	128-bits, with 16 iterations	Message authentication and message digest	

¹ All new implementations of MACs and hashes MUST not be based on MD5.

Algorithm	Minimum Key Length	Appropriate Usage
SHA-1 ²	Not applicable.	Message authentication and message digest
SHA-2	Not applicable	Message authentication and message digest
TDES (Triple DES) MAC	112-bits	Message authentication
Digital Signatures		
DSA (Digital Signature Algorithm)	1024-bits	Digital Signature
Elliptic Curve DSA	160-bits	Digital Signature
RSA DSA	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	1024-bits	Digital Session key establishment
Elliptic Curve Diffie-Hellman	160-bits	Digital Session key establishment
Cryptographic Protocols		

² All new implementations of MACs and hashes MUST not be based on SHA-1.

Algorithm	Minimum Key Length	Appropriate Usage
TLS 1.1 and higher	N/A	Protocol to authenticate and encrypt communication between authenticated parties

5.7 Appendix G: 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)	<ul style="list-style-type: none"> • Instances of detected malware • File and information system disinfection attempts • File quarantines • Malware scans • Signature or software updates
Intrusion detection and intrusion prevention systems	<ul style="list-style-type: none"> • Suspicious behaviour • Detected attacks • Actions performed to stop malicious activity
Remote access and wireless access systems	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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))	<ul style="list-style-type: none"> • System Events <ul style="list-style-type: none"> • System shut down • Service starting 	<ul style="list-style-type: none"> • Security Events <ul style="list-style-type: none"> • 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 Security Logging and Monitoring section for EMR Offering application-level (PHI) logging and auditing requirements.	<ul style="list-style-type: none"> • Client requests and server response • Authentication attempts • Account changes • Use of privileges • Number and size of transactions • Operational events • Start-up and shutdown 	<ul style="list-style-type: none"> • Configuration changes • Application-specific events such as: <ul style="list-style-type: none"> • Email sends and receipts • File access • Service request • System-level transactions • A function performed (such as read, write, modify, delete)