BRITISH COLUMBIA | Ministry of Health

British Columbia
Professional and Software Conformance Standards

Electronic Health Information Exchange

Volume 9: Information Privacy and Security

Version1.2 2015-05-29

Security Classification: Low Sensitivity

Copyright Notice

Disclaimer and Limitation of Liabilities

This document and all of the information it contains is provided "as is" without warranty of any kind, whether express or implied. All implied warranties, including, without limitation, implied warranties of merchantability, fitness for a particular purpose, and non-infringement, are hereby expressly disclaimed.

Under no circumstances will the Government of British Columbia be liable to any person or business entity for any direct, indirect, special, incidental, consequential, or other damages based on any use of this document, including, without limitation, any lost profits, business interruption, or loss of programs or information, even if the Government of British Columbia has been specifically advised of the possibility of such damages.

Author:	MOH Health Information Privacy and Security Branch
Date Created:	Date
Last Updated:	2015-05-29
Version:	1.2

Table of Contents

Tables

1.0 Introduction

Organizations developing interfaces to *health information exchange (HIE) services* offered by the Ministry of Health (the "ministry") must meet the British Columbia Professional and Software Conformance Standards (the "Conformance Standards") which the Ministry publishes.

The Ministry's Conformance and Integration Services team will facilitate the registration, connection, conformance testing and certification processes required for applications to connect to the ministry HIE services.

1.1 Conformance Standards Volume Set

The Conformance Standards are the central reference for organizations wanting to integrate their *Points of Service (POS)* applications with Ministry HIE services. This integration will allow their users to exchange important demographic and clinical information with other health care professionals in support of efficient and safe patient care. The Conformance Standards contain multiple volumes and must be reviewed as a complete set.

The volumes in the Conformance Standards are divided into topics such as: business rules, application-enforced rules, change management rules, privacy and security rules, and technial message and transport specifications. The Conformance Standards are available on the Conformance and Integration Services website: http://www.health.gov.bc.ca/access/software_development.html.

1.2 Key to Document Terminology

The Conformance Standards in this volume use a consistent language convention:

- The word "should" is used to indicate a recommended requirement meaning that the standard is optional (i.e., not compulsory yet encouraged). Conformance testing, service on-boarding activities and/ or application testing will confirm that this standard is correctly implemented where appropriate.
- All other standards or rules as stated are a compulsory function or requirement. The words "must" "will", "minimum", or "mandatory" are used to indicate this. Conformance testing, service on-boarding activities and/ or application testing will confirm that this standard is correctly implemented.
- Acronyms and abbreviations are used for repetitions of some system and organization names. The first time an acronym or abbreviation appears in the document it is accompanied by the full name.

A Glossary of Terms is provided in a separate volume of the Conformance Standards. Each defined term, acronym and abbreviation that is included in the glossary is italicized in the Conformance Standards the first time it appears in the volume.

1.3 Purpose of Document

This document describes the the Information Privacy and Security requirements for software organizations developing POS systems used to access HIE services in the *custody*, or under the control of the Ministry of Health (the "ministry") for the delivery of health care services in the Province of British Columbia.

The ministry conformance team uses this material to ensure that POS systems comply with the Conformance Standards. POS systems will be tested for conformance against the rules in this document.

1.4 Intended Audience

The intended audience for this document is:

- **Information Consumers** – who access electronic health information from a Ministry or provincial *data repository* (e.g., end users);
- **Information Custodians** – who maintain or administer *electronic health information* (EHI) resources on behalf of the Information Authority;
- **Information Authority** – who have the responsibility and decision making authority for EHI throughout its lifecycle, including creating, classifying, restricting, regulating, and administering its use or disclosure;
- **Data Providers** – who provide data to, or exchange data with a Ministry data repository (e.g., system to system upload);
- **Software Organizations** – organizations (including in-house system development teams) who develop interfaces to health information exchange systems and/or support those interfaces;
- **Conformance Team(s)** – who are responsible for evaluating and testing conformance, including organizational security practices and business processes; and
- **Audit Team(s)** – who are responsible for independent examination and evaluation of compliance including organizational security practices and business processes.

1.5 Ministry of Health Conformance Standards Contact

For more information regarding the Conformance Standards, questions should be directed to Conformance and Integration Services at: HLTH.CISSupport@gov.bc.ca

2.0 Information Privacy and Security

The rules in this volume define the mandatory standards for a point of service software organizations.

Each standard will be evaluated, as indicated in the evaluation column of each table, by one or more of the following processes:

- (A) Attest by signing the Vendor Participation Agreement that your product conforms to the stated standard and that documented policy and procedures are maintained for internal purposes or to support an audit;
- (C) Attest to as indicated in (A) and provide a comment. The comment must provide a high-level description of how your product conforms to the stated standard (see Guidance column for more information); and
- (D) Attest to as indicated in (A) and demonstrate that your product conforms to the stated standard.

2.1 General Privacy and Security

This section describes the information privacy and security rules that apply to all software solution providers.

Table 1 General Privacy and Security Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS1.1	**Use of Production Environment** The production environment (i.e., the operational information system) must not be used for application development, testing or training.	A	
PS1.2	**Change Management** A formal and structured change management process (i.e., ITIL Best Practices for Service Management) must be used with procedures to control the implementation of software and upgrades and patches/hot fixes including security patches for system components and software.	A	
PS1.3	**Access, Disclosure and Storage Outside of Canada** Access to, disclosure, and storage of electronic health information must be within Canada unless permitted in writing by the ministry in accordance with applicable laws.	A	
PS1.4	**Personnel Restricted Data Access**	A	

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
	Processes and procedures must be in place to ensure that access to EHI data by personnel and subcontractor personnel is based strictly on role and need to know to maintain operations.		
PS1.5	**Least Privilege Access** Employ a least privileges model for the user and service accounts that run the application. The application must run at the user privilege level and not system/root level.	C	Provide a high-level description of application security features.
PS1.6	**Authentication Settings** All default authentication settings for high-level privileged accounts (e.g., those used to perform application administration) must be changed before the application is fully deployed.	C	Provide a copy of the application deployment procedure.

3.0 Application Development

This section describes the information privacy and security rules that apply to all organizations developing health information technology systems and applications to access or exchange EHI with any ministry system or data repository.

3.1 Secure Development

Table 2 Secure Development Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS2.1	**Development Lifecycle** The organization must follow an application development life cycle methodology, which addresses information security throughout the phases of the Secure System Development Life Cycle.	C	Provide a high-level description of the Secure System Development Life Cycle followed.
PS2.2	**System Coding** a) The organization must comply with good practice for system coding (e.g., using structured programming techniques, creating code that is modular, and documenting code); b) Insecure design techniques must not be used (e.g., must not hard code passwords, hostnames, IP addresses, encryption keys into source code); c) Development tools, such as integrated development environments, must be configured to help enforce the creation of secure code; and d) Source code must be protected from unauthorized access and tampering (e.g., by using configuration management tools, which typically provide features such as access control and version control).	C	Provide a high-level description of the practices followed.
PS2.3	**Environment Segregation** Development, testing and training environments must be segregated from production environments.	C	Provide a high-level description of development, test, and training environments.
PS2.4	**Personnel Assignments** There must be a separation of duties between personnel assigned to develop software in	C	Provide a high-level description for personnel

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
	development environments and those assigned to maintain software in production environments.		assignments.
PS2.5	**Inactive Test Accounts** A test account inactive (or not activated) for greater than 45 days is considered dormant and must be: a) Removed from the system; or b) Disabled to prohibit login to the system.	C	Provide a high-level description for test account procedures.
PS2.6	**Test Data** If test data contains personal or sensitive information, the personal or sensitive information must be removed, depersonalized or modified beyond recognition before the test data can be used. The test data must be removed once testing is complete.	C	Provide a high-level description for test data procedures.
PS2.7	**Application Modification** The ministry must be notified when the application has been materially modified, enhanced or updated where upon the application will be conformance tested at the discretion of the ministry.	A	

3.2 Application Audit Functionality

Table 3 Application Audit Functionality Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS3.1	**Logging Access** The application must create a time stamped audit record each time a user (including all privileged users, such as system administrators): a) Accesses, creates or updates electronic health information; and b) Logs in or out of the system. Note: The application should have the capability to provide audit logs to a Security Information and Event Management (SIEM) tool.	D	

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS3.2	**Minimum Content of Audit Logs** The application must record, at minimum, the following information for each event: a) User identification; b) User role; c) Date and time; d) Success or failure indication; e) Origin of event (e.g., health organization, informational custodian, physical/departmental location or virtual location/identifier), f) Originating IP address; g) Domain or repository accessed; h) Type of event, activity or function performed (e.g., create, view, update, print); i) Type, identity or name of affected data, system component, or resource; and, j) Transaction number or ID. The application must minimize the amount of personal health information (PHI) recorded in audit logs to protect patient privacy and to meet legislative or regulatory requirements.	D	
PS3.3	**Audit Log Retention** Audit logs must be retained for a minimum of two years.	C	Provide a description of the archiving feature.
PS3.4	**Access Audit Reports** The application must be capable of generating user defined reports to provide, at a minimum: a) Reports by patient: Identifying all users who have accessed or modified a given patient's record(s) over a given time; and b) Reports by user: Identifying all records accessed or modified by a given user over a given period of time.	D	

3.3 Application Accounts and System Access

Table 4 Application Accounts and System Access Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS4.1	**Account Lock Out** An account lockout threshold must be set to a maximum of six consecutive failed attempts. After reaching an account lockout threshold the logon process must: a) Lock the account and require administrator intervention; or b) Lock the account for a minimum of 15 minutes and then reset the account lockout counter back to zero.	D	
PS4.2	**Access Control** The application must incorporate an effective security scheme that will: a) Control system access (by adding or removing/disabling user identifiers); b) Uniquely identify the user by user IDs; and c) Require authentication for system access such as a userID and password or two-factor token (preferred). Note: Ministry system authentication requirements such as referencing/using external federated authentication solutions have yet to be determined.	C/D	Provide a high-level description of the application's access control features.
PS4.3	**Privileged User Access** A privileged user ID, defined as having the ability to control security access and other restricted system functions, must not have the ability to access the EHR.	C/D	Provide a high-level description of privileged user access control features
PS4.4	**Multi-factor Authentication** When multi-factor authentication is used, the associated password, passphrase or passcode must be a minimum length of 6 characters. Note: Passwords, passphrases or passcodes should be changed at least annually.	D	
PS4.5	**Role Based Access** The application must support role-based access controls which can: a) Map a user to one or more roles; b) Map each role to one or more system functions; c) Create new roles; and d) Restrict/ limit access to system function or data based on role.	C/D	Provide a high-level description of the role management features and documented Role-based Access Model followed.

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS4.6	**Single Role per Session** If a user ID supports multiple roles, the application must: a) Prompt the user to select from the assigned roles, and b) Apply the permissions for only the selected role. The user ID must not be given aggregate permissions for all of their assigned roles.	D	
PS4.7	**Role-based Functionality** The application must provide and restrict functionality in full accordance with the user's business role and user's provincial EHR Service business role.	D	
PS4.8	**Secure Sign-on Configuration** The application must securely manage user sessions by: a) Validating sign-on information only when it has all been entered; and, b) Limiting the duration of any one sign-on session.	C/D	Provide a high-level description of user session controls.
PS4.9	**Sign-on Display and Warnings** Application sign-on mechanisms for user sessions must be configured so they: a) Do not display specific electronic health information details until after sign-on is completed successfully; and b) Warn that only authorized users are permitted access.	D	
PS4.10	**Session Inactivity** The application must clear the screen of personal and confidential information when a session has been inactive after a configurable period (maximum of 15 minutes). (e.g., locking screensavers or automatic disconnection of inactive sessions) The screen must remain clear of personal and confidential information until an authorized user successfully enters a valid user ID and password, or two-factor credentials.	D	
PS4.11	**Managing User Passwords** The application must use the following password management features:	D	

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
	a) Passwords are not displayed on screen or on print-outs; b) Temporary passwords issued to users are changed on first use; c) New passwords are verified before the change is accepted; d) Users set their own passwords and can change them at any time; e) A password complexity setting; f) A password change frequency setting; g) Upon password expiration, the user is instructed (forced) to immediately assign a new password; and h) A password history setting where re-use of passwords is restricted (i.e., so the password cannot be used again within a set period or set number of changes).		
PS4.12	**Password Protection** Passwords must be protected (i.e., not sent/stored in clear text) when transmitted or stored by the application. Each password must be individually protected with one of the following methods: a) Concatenate the password to a salt or nonce and/or username, then hash (SHA-256); or b) Encrypt the password with a keyed encryption algorithm (AES-256), or c) An alternate technical solution submitted to and approval by the Province.	C/D	Provide a high-level description of the applicable security feature.
PS4.13	**Sign-on Mechanism and Passwords** Accounts, user IDs, and passwords must not be embedded in the source code or in automated (batch) routines.	D	
PS4.14	**Remote Access to the Application** Remote access to the application must have in place the following controls: a) Secure remote access technologies such VPN, firewall rules, authentication, encryption (minimum AES-128 bit); b) Audit and monitoring processes during the remote access sessions; c) Automatic disconnect of sessions after a specific period of inactivity;	C	Provide a high-level description of remote access controls.

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance

	d) Unique identifiable user IDs;
	e) Multi-factor authentication;
	f) Devices that meet minimum security configuration (e.g., up-to-date malware protection, latest systems and software patches installed, personal firewall); and
	g) Accessed from a location within Canada, unless otherwise permitted in writing by the ministry in accordance with applicable laws.		

PS4.15	**Inactive User Accounts** A user account inactive (or not activated) for 90 days or greater is considered dormant and must be disabled to prohibit login to the system.	D	

3.4 Patient's Protective Word

A patient's Protective Word is a password chosen by the patient, used to control access to the patient's electronic health record. Protective Words are assigned through two mechanisms:

- A patient initiated Disclosure Directive to protect their EHR data in the Provincial Laboratory Information Solution, and
- A patient initiated request through a pharmacist or HIBC to protect their EHR data in the PharmaNet system.

Table 5 Patient's Protective Word Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS5.1	**Securing Patient's Protective Word** Protective words stored in the POS application must be individually protected by one of the following methods: h) Encrypt the protective word with a keyed encryption algorithm (AES-256); or i) An alternate technical solution submitted to and approved by the Province.	C/D	Provide a high-level description of the Protective Wword protection scheme used.

3.5 Application Coding

Table 6 Application Coding Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS6.1	**Protecting Against Unauthorized Access** The application must be protected against unauthorized access to information by: a) Employing secure defaults (including logging is active by default); b) Ensuring key components 'fail securely' (i.e., in the event of a system failure, information is not accessible to unauthorized individuals, and cannot be tampered with or modified); and, c) Not disclosing information about its internal workings (e.g., in application responses or error messages).	C	Provide a high-level description of application security features.
PS6.2	**Secure Coding Requirements** Application code must be tested and remediated for, at a minimum, the common coding vulnerabilities: a) Injection flaw; b) Buffer overflow; c) Insecure cryptographic storage; d) Insecure communication; and e) Improper error handling.	C	Provide report of test and any required remediation.
PS6.3	**Code Review** Application code must be reviewed prior to release to production in order to identify any potential coding vulnerability. Note1: Code reviews should be performed by individuals other than original code author. Note 2: Code reviews should be performed by individuals who are knowledgeable in code review techniques and secure coding practices.	C	Provide details on when and who performed the final code review.
PS6.4	**Cryptographic Keys** Cryptographic keys stored within the application must be protected.	C	Provide a high-level description of security features.
PS6.5	**Electronic Health Information Transmission** The application must apply cryptographic algorithms and protocols during transmission of electronic health information when:	C	Provide a high-level description of interface architecture and

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
	a) The data is transmitted beyond a single physical network; and b) The network is shared by more than one business entity. Note: The application should be designed to accept future cryptographic specifications or requirements of ministry systems.		related security features.
PS6.6	**Data Retention** Data must be retained for a defined period of time as required by applicable laws, bylaws and regulations.	C	Provide a high-level description of the archiving feature.

3.6 Web Application

Table 7 Web Application Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS7.1	**Protecting Against Data Corruption or Disclosure** Information used by web applications (e.g., configuration files) must be protected against corruption or unauthorized disclosure by: a) Using partitions inaccessible to web servers (or other connected servers); b) Restricting file permissions; and c) Encrypting all the connection strings stored on the web server.	C	Provide a high-level description of security features.
PS7.2	**Preventing Information Leakage** The unauthorized disclosure of system configuration information (that could be useful to hackers) must be prevented by, at a minimum: a) Suppressing or modifying the server field in HTTP headers that identify the web server's brand and version; b) Verifying that directories of files on web servers are not indexable; c) Preventing source code of server-side executables and scripts from being viewed by a web browser; d) Ensuring that the source of HTML, JavaScript and other client-side scripting languages does not contain unnecessary information (e.g.,	C	Provide a high-level description of security features.

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
	comments and details of functions); and e) Using the POST method when submitting all sensitive form data.		
PS7.3	**Recording Actions** Public-facing web servers that support the web application must be configured to: a) Record actions performed (e.g., those associated with server-side executables and scripts); and b) Log security-related events generated by the website.	D	
PS7.4	**Web Application Vulnerabilities** Application code used for web applications and application interfaces must be tested and remediated for, at a minimum, the following web application and application interface vulnerabilities: a) Cross-site scripting (XSS); b) Improper access control; and c) Cross-site request forgery (CSRF).	C	Provide report of final test including any required remediation.
PS7.5	**Storing Electronic Health Information** The web application must not store electronic health information or sensitive information in hidden form fields or unencrypted cookies.	C	Provide a high-level description of security features.
PS7.6	**Protecting Web Sessions** Web application sessions must be protected by: a) Ensuring session IDs cannot be easily predicted (e.g., using randomly generated session IDs); b) Configuring the security parameters in ‘cookies’ used to hold session information; c) Encrypting network traffic (e.g., SSL) between the web browser and the web server and between the web server and the database; and d) Setting sessions to expire after inactivity (HTTP timeout to a maximum of 15 minutes) and after a set length of time (absolute timeout to the minimal value possible depending on the context of the web application).	C/D	Provide a high-level description of interface architecture and related technical security features.
PS7.7	**Application Scanning** Application vulnerability assessments (automated	C	Provide a high-level description of the application scanning

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
	tools or manual methods) must be used to validate that the web application is not susceptible to known vulnerabilities. Alternatively, or additionally, a web-application firewall configured to provide protection from known attacks can be used. Note: A web-application firewall is a firewall specialized to protect Web servers from malicious traffic and blocks attempts to compromise the system. It prevents targeted attacks that include application layer DoS attacks cross-site scripting, SQL injection, forceful browsing, cookie poisoning and invalid input.		procedure and details of when and who performed the final application scan.

4.0 Application Support

This section describes the information privacy and security requirements for those *software* solution providers who provide application support for health information technology systems.

4.1 Organizational Policy

Table 8 Organizational Policy Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS8.1	**Governance** Organizational structures must be established and responsibility assigned to identified individuals to ensure compliance with privacy and security requirements. Note: Sources for developing governance structures, may include, but are not limited to: • ISO 27001 - Information Security Management Systems Requirements; • ISO 27002 - Code of Practice for Information Security Management • ISO 27799:2008 - Information Security Management in Health; and • The Canadian Standards Association's Model Code for the Protection of Personal Information (CAN-CSA-Q830-03).	C	Provide a high-level description of the information privacy and security organizational structure and list individuals responsible.
PS8.2	**Policies and Procedures** Privacy and security policies and procedures must be established (or adopted) and published, including policies and procedures related to secure storage, retention, transport and disposal of client data records; audit log reviewing; and user account maintenance. Note: Sources for developing policies and procedures, may include, but are not limited to: • ISO 27001 - Information Security Management Systems Requirements; • ISO 27002 - Code of Practice for Information Security Management; • ISO 27799:2008 - Information Security Management in Health; and • The Canadian Standards Association's Model Code for the Protection of Personal	A	

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
	Information (CAN-CSA-Q830-03).		

4.2 Staff and Contractors

Table 9 Staff and Contractors Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS9.1	**Confidentiality Agreements** All personnel (employees and contractors) who access or support the application must sign a confidentiality agreement that is renewed annually with the organization.	C	Provide a copy of HR policy requiring a signed confidentiality agreement and a sample agreement.
PS9.2	**Acceptable Use Agreements** All personnel (employees and contractors) who access or support the application must sign an acceptable use agreement which defines user responsibilities for software, computer equipment, network, and internet use.	C	Provide a copy of HR policy requiring a signed acceptable use agreement and a sample agreement.
PS9.3	**Privacy and Security Awareness Training** All personnel (employees and contractors) who access or support the application must regularly receive information privacy and security awareness training which includes the privacy and security requirements in this document.	C	Provide a copy of HR policy requiring staff to take privacy and security training.

4.3 Complaints and Incidents

Table 10 Complaints and Incidents Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS10.1	**Information Incident Management** Procedures must be established for managing suspected and actual information incidents to meet, at minimum, the requirements recommended by the Office of Information and Privacy Commissioner for British Columbia. Note: An information incident is when unwanted or unexpected events happen that threaten privacy or information security. Information	A	

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
	incidents are also called privacy breaches when they involve personal information about people, such as names, birthdates, social insurance numbers, or client file information. A breach can include the loss or theft of personal health information or other unauthorized activities, including unauthorized access that may result in the loss of custody or control over personal health information.		
PS10.2	**Information Incident Reporting to the Ministry** Suspected or actual information incidents or breaches that involve electronic health information must be immediately reported to the ministry in accordance with the terms and conditions of applicable agreements.	A	
PS10.3	**Whistle-Blower Protection** Personnel (employees and contractors) must be aware of procedures for responding to suspected and actual privacy and security incidents and breaches, including "whistle-blower" protection measures.	C	Provide a copy of the procedures followed that demonstrates whistle-blower protections.

4.4 Technical Support

Table 11 Technical Support Rules

#	Rule	**E**valuation **A**ttest **C**omment **D**emonstrate	Guidance
PS11.1	**Remote Technical Support Sessions** Support sessions provided via remote-access technologies must be: a) Delivered using software that requires and logs the client's approval prior to the remote take over; b) Monitored when in use; and c) Encrypted (at a minimum AES-128 bit).	A	
PS11.2	**Storing of Data Prohibited** When providing remote technical support via remote-access technologies, the copy, move, and storage of data onto local hard drives and removable electronic media must be prohibited.	A	

#	**Rule**	**E**valuation **A**ttest **C**omment **D**emonstrate	**Guidance**
PS11.3	**VPN Remote Support** When providing remote technical support using a VPN for remote access, split tunneling must be disabled at the technical support agent's workstation while the technical support session is active.	A	

5.0 Application and Data Hosting Services

5.1 Application and Data Hosting Environment

This section describes the information privacy and security requirements for health information technology systems' application and data hosting services- systems hosted by an Application Service Provider (ASP).

Organizations that develop and operate applications for medical practices, commonly referred to as electronic medical record (EMR) systems, must be hosted by an application service provider. Medical practice EMR systems must be hosted by an application service provider (ASP). EMR systems not hosted by an ASP will not be permitted to connect to the ministry’s health information exchange systems.

An ASP provides network-based access to software services and involves:

- Remotely hosting a client’s system, application and data on its secured computer servers.
- Providing client access through a web browser or thin client.
- Professionally managing the servers and other related technologies.
- No POS client server hardware or software being required at the point of care.

Table 12 Protection of the Application and Data Hosting Environment Rules

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
PS12.1	**Physical and Environmental Protection** Policy and procedures that address the purpose, scope, roles, responsibilities, and compliance for physical and environmental security including security perimeter and entry controls, working in secure areas, equipment security, cabling security, fire detection and suppression, room temperature controls, and flood/water hazard must be in place.	A	
PS12.2	**Secure Area** Areas that house equipment (e.g., server rooms, network or telecommunications closets) must be protected against unauthorized access by using the following physical security measures: a) Strong physical security perimeter by using solid construction walls, alarmed fire doors, and armoured windows; b) Locks activated by keypads, swipe cards or equivalent;	C	Identify and briefly describe all computer rooms, data centers and other physical areas that house systems and for each area identified describe the physical security controls.

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
	c) Intruder alarms; d) Security guards; and e) Recorded video surveillance.		
PS12.3	**Physical Access Monitoring** Physical access to the secure areas (and the systems within the secure areas) in the application hosting environment must be monitored. Records for approved personnel access and sign-in sheets for visitors must be maintained. Logs must be periodically reviewed, violations or suspicious activities investigated, and action is taken to address issues.	A	
PS12.4	**Protecting Equipment** Equipment including data or software for supporting the application hosting environment must: a) Only be repaired or serviced by authorized personnel; and b) Not be removed or taken off premises without prior authorization by management.	C	Provide a copy of the policies and procedures followed.
PS12.5	**On-site Technical Support Services** Personnel involved in on-site technical support must be monitored/ escorted while in restricted access areas.	A	
PS12.6	**Environmental Controls** Environmental controls must be provisioned and properly maintained, including but not limited to: 1. Uninterrupted power supply to facilitate an orderly shutdown process; 2. Fire detection and suppression; 3. Temperature and humidity controls; and 4. Water damage detection and mitigation.	C	Identify and briefly describe all environmental controls.

5.2 Auditing

Table 13 Auditing Rules

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
PS13.1	**Access Audit Program** Audit and control procedures must be in place to monitor the activities for all support services and personnel within the application hosting environment. The access audit program may: a) Integrate into existing random audit processes; b) Integrate into existing proactive audit reporting; or c) Be established as a new process. Minimum review requirements must be set, including regular review of standard and routine reports, regular random audits/ spot checks, and proactive measures. There must be a designated individual(s) in the organization with the responsibility for access audit. The responsibility must include providing evidence to auditors and oversight authorities that the reviews have been completed.	A	
PS13.2	**Reporting to Management** Audit logs and exception reports produced from audit logs must be regularly reviewed and the findings communicated to management, including: a) Any unusual patterns or anomalies; and b) Potential security weaknesses or breaches.	A	
PS13.3	**Integrity of Log Files** Audit logs (including any backup copies) must be secured so that the information contained within them cannot be altered.	C	Provide a high-level description of security measures.
PS13.4	**Audit Log Retention** Audit logs must be retained for a minimum of two years.	C	Identify the retention period.
PS13.5	**Audit Log Restrictions** Access to the audit logs and audit tools must be restricted to authorized personnel to prevent misuse or compromise.	C	Provide a high-level description of security measures.
PS13.6	**Audit Trails** A process for linking all access to system	C	Provide a list and description of the

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
	components (especially access done with administrative privileges such as root) to each individual user must be established.		enabled audit trails for system components.
PS13.7	**Audit Events** Automated audit trails must be implemented for all system components to reconstruct the following events: a) All individual accesses to application hosting environment data; b) All actions taken by any individual with root or administrative privileges; c) Access to all audit trails; d) Invalid logical access attempts; e) Use of identification and authentication mechanisms; f) Initialization of the audit logs; and g) Creation and deletion of system-level objects.	C	Provide a high-level description on how individual access events are logged.
PS13.8	**Audit Record Fields** Audit trail entries must record at least the following for all system components for each event: a) User identification; b) Type of event; c) Date and time; d) Success or failure indication; e) Origin of event; and f) Type, identity or name of affected data, system component, or resource.	C	Provide a high-level description of audit trail entries recorded for events logged.
PS13.9	**Network Time** All system components that support the application hosting environment must use time-synchronization technology (NTP) to synchronize system clocks. The following must be implemented for acquiring, distributing, and storing time: a) Time data is protected; and b) Time settings are received from industry-accepted time sources (e.g., NIST http://nist.time.gov/)	C	Provide a high-level description of how time-synchronization technologies are implemented.

5.3 Accounts and Systems Access

Table 14 Accounts and Systems Access Rules

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
PS14.1	**Account Lock Out** After reaching an account lockout threshold (maximum of six consecutive failed logon attempts) for a privileged account, the logon process must lock the account and require administrator intervention.	A	
PS14.2	**Distribution of Passwords** Passwords/passphrases must be securely communicated and separate from the user ID when transmitted electronically.	A	
PS14.3	**Multi-factor Authentication** Multi-factor authentication must be used for access to the application hosting environment by employees, administrators, and third parties. Associated password/passphrase must be a minimum length of 6 characters or digits in the case for a passcode. Note: Passwords, passphrases or passcodes should be changed at least annually.	C	Provide a high-level description of authentication method used.

5.4 Hardware and Peripherals

Table 15 Hardware and Peripherals Rules

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
PS15.1	**Restricting Access to Unattended Management Consoles** Screens on unattended management consoles must be cleared after a set period of inactivity (maximum of 15 minutes) and requires signing on again with a password before restoring screens.	C	Provide a high-level description of security measures.
PS15.2	**Malware Protection** Anti-virus software must be deployed on all systems commonly affected by malicious software (particularly servers in the DMZ). Anti-virus mechanisms must be current, actively running,	C	Provide a high-level description of security measures.

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
	and generating audit logs.		
PS15.3	**Computing Devices Connecting to the Internet** Computing devices used for the management of application hosting environment servers must not have direct connectivity to the internet.	C	Provide a high-level description of security measures.
PS15.4	**Limit Use of Mobile and Portable Storage Devices** Mobile and portable storage devices (e.g., external hard drives, USB flash drives, CDs, including wireless devices) that may be used to copy or remove electronic health information must not be permitted within the application hosting environment.	C	Provide a copy of the policy.
PS15.5	**Security Patching** A patch management process must be followed in applying security patches for application hosting environment system components and software that access/ exchange electronic health information. Critical security patches must be applied in a timely manner, unless there is a technical or business reason why the patches cannot be applied. In situations where a security patch cannot be readily applied, a mitigating strategy must be developed and implemented.	C	Provide a copy of policy and procedures.
PS15.6	**Secure Disposal of Equipment** All Personal Health Information must be permanently removed from computer equipment prior to disposal of the equipment.	C	Provide a copy of policy and procedures.

5.5 Network

Table 16 Network Rules

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
PS16.1	**Remote Access** Remote access to application hosting environment servers is only permitted when a service provider requires access to perform technical support services. The following controls must be in place for the remote technical	C	Provide a copy of the policy.

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
	support: a) Secure remote access technologies such VPN, firewall rules, authentication, encryption (minimum AES-128 bit); b) Audit and monitoring processes during the remote access sessions; c) Activation of remote-access technologies only when needed with immediate deactivation after use; d) Automatic disconnect of sessions after a specific period of inactivity; e) Approved and logged on a case by case basis; f) Unique identifiable user IDs; g) Multi-factor authentication; h) Devices that meet minimum security configuration (e.g., up-to-date malware protection, latest systems and software patches installed, personal firewall); and i) Provided from a location within Canada, unless otherwise permitted in writing by the ministry in accordance with applicable laws.		
PS16.2	**Limiting Wireless Networks** Wireless networks must not be used within the application hosting environment.	C	Provide a copy of the policy.
PS16.3	**Firewall and Router Configuration** Firewall and router configuration standards must be established and include the following: a) Formal process for approving and testing all network connections and changes to the firewall and router configurations; b) Current network diagram with all connections to application hosting environment data; c) Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone; d) Description of groups, roles, and responsibilities for logical management of network components; e) Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure (e.g., FTP, Telnet, POP3, IMAP, and SNMP); and	A	

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
	f) Requirement to review firewall and router rule sets at least every six months.		
PS16.4	**Firewall and Router Controls** Firewall and router configurations must restrict connections between untrusted networks and any system components in the application hosting environment. a) Limit inbound and outbound traffic to that which is necessary for the application hosting environment; and b) Secure and synchronize router configuration files. Note: An "untrusted network" is any network that is external to the application hosting environment under review, and/or which is out of the ASP's ability to control or manage.	A	
PS16.5	**Restrict Direct Public Access** Direct public access between the Internet and any system component in the application hosting environment must be prohibited. The following must be implemented: a) A DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; b) Limit inbound Internet traffic to IP addresses within the DMZ; c) Do not allow any direct connections inbound or outbound for traffic between the Internet and the application hosting environment; d) Connections to the application hosting environment utilizing the Internet must be protected using a reverse proxy in the DMZ; e) No "split-tunneling" of any secure connection between the application hosting environment and client; f) Do not allow internal addresses to pass from the Internet into the DMZ; g) Do not allow unauthorized outbound traffic from the application hosting environment to the Internet; h) Implement stateful inspection, also known as dynamic packet filtering (i.e., only established connections are allowed into the network); i) Place system components that store	A	

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
	application hosting environment data (e.g., a database) in an internal network zone, segregated from the DMZ and other untrusted networks; j) Do not disclose private IP addresses and routing information to unauthorized parties. Notes: Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT); • Placing servers containing application hosting environment data behind proxy servers/firewalls or content caches; • Removal or filtering of route advertisements for private networks that employ registered addressing; and • Internal use of RFC1918 address space instead of registered addresses.		
PS16.6	**Restricting Access to Network Devices** Network devices, including network diagnostic ports and services, must be restricted to authorized network staff using access controls that support individual accountability, and be protected from unauthorized access.	A	
PS16.7	**Host System Protection** Vendor-supplied defaults must be changed before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	A	
PS16.8	**Host System Configuration** Configuration standards must be developed for all system components. These standards must address all known security vulnerabilities and be consistent with industry-accepted system hardening standards. Note: Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS); • International Organization for Standardization (ISO); • SysAdmin Audit Network Security (SANS) Institute; and • National Institute of Standards Technology (NIST).	A	

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
PS16.9	**Host Primary Function** There must be only one primary function per server (e.g., web servers, database servers, and DNS must be implemented on separate servers). Where virtualization technologies are in use, implement only one primary function per virtual system component. Note: This is to prevent functions that require different security levels from co-existing on the same server.	A	
PS16.10	**Limit Host Services** Host system services must be limited to only necessary and secure services, protocols, daemons, etc., as required for the function of the system. a) Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers; b) Implement security features (e.g., SSH, S-FTP, SSL, or IPSec VPN) for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, file-sharing, Telnet, FTP); and c) Configure system security parameters and set according to configuration standards to prevent misuse.	A	
PS16.11	**Segregate Client Organization** Each client organization hosted within the application hosting environment must be segregated by: a) Ensuring that each client organization only runs processes that have access to that client's data environment; b) Restricting each client organization's access and privileges to its own data environment only; c) Ensuring that logging and audit trails are enabled and unique to each client's data environment; and d) Enabling processes to provide for timely forensic investigation in the event of a compromise to any client's data.	A	
PS16.12	**System Utility Program Controls** The use of system utility programs (which may be used to override system and application	A	

#	Rule	Evaluation Attest Comment Demonstrate	Guidance
	controls) must be restricted and tightly controlled (i.e., utilities are managed/monitored on use, and access based on role and segregation of duty).		
PS16.13	**Encrypt Non-console Communications** Strong cryptography must be used to encrypt all non-console administrative (network) access. Technologies (e.g., SSH*,VPN, or TLS**) for web-based management and other non-console administrative access must be used. *SSH v2.0 or higher with AES-256 ** TLS v1.2 or higher with AES-128	C	Provide a high-level description of security measures implemented.
PS16.14	**Intrusion Prevention and Detection** Intrusion-detection systems, and/or intrusion-prevention systems must be used to monitor all traffic at the perimeter of the application hosting environment as well as at critical points inside of the application hosting environment, and alert personnel to suspected compromises. All intrusion-detection and prevention engines, baselines, and signatures must be kept up-to-date.	C	Provide a high-level description of security measures implemented.
PS16.15	**Disaster Recovery Security Controls** During disaster recovery, the backup application hosting environment must have the same security controls as the primary application hosting environment.	C	Provide a high-level description of security measures implemented.
PS16.16	**Backup Files Stored Offsite** Backup files stored offsite, must be encrypted to AES-256 or stronger. The offsite storage location's security must be reviewed annually.	C	Provide a high-level description of security measures implemented.