Pharmacy Practice Management Systems:

Requirements to Support NAPRA's "Model Standards of Practice for Canadian Pharmacists"

November 2013

NAPRA ANORP

National Association of Pharmacy Regulatory Authorities
Association nationale des organismes de réglementation de la pharmacie

Pharmacy Practice Management Systems: Requirements to Support NAPRA's "*Model Standards of Practice for Canadian Pharmacists*"

Approved by the National Association of Pharmacy Regulatory Authorities' (NAPRA) Board of Directors April 2013, published November 2013.

The National Association of Pharmacy Regulatory Authorities (NAPRA)
220 Laurier Avenue West, Suite 750, Ottawa, ON K1P 5Z9
E-mail: info@napra.ca | Telephone: (613) 569-9658 | Fax (613) 569-9659

NAPRA ANORP
National Association of Pharmacy Regulatory Authorities
Association nationale des organismes de réglementation de la pharmacie

Executive Summary

The information management systems used by pharmacy professionals (referred to in this document as pharmacy practice management systems or PPMS) must support the delivery of patient care including the dispensing of drugs in accordance with Canadian regulations and standards. They must also do much more: the ability to record, display, store, and exchange patient specific information in a manner that optimizes workflow within pharmacy teams is critical. PPMS must facilitate both information exchange with external systems such as electronic health record systems and also processes such as electronic prescribing, while simultaneously preserving the confidentiality and security of all personal health information processed or transmitted.

Pharmacy regulatory authorities have a responsibility to consider the minimum requirements of systems used by pharmacists and pharmacy technicians in their delivery of quality care and services. The Council of Pharmacy Registrars of Canada (CPRC), an advisory committee of the National Association of Pharmacy Regulatory Authorities (NAPRA) established a working group for this purpose to be informed by the "Model Standards of Practice for Canadian Pharmacists"[1] developed by NAPRA and the Pan-Canadian Drug Messaging Standard[2] developed by Canada Health Infoway. These requirements will be instructive to pharmacists, pharmacy managers, pharmacy owners, vendors, and the developers of federal/provincial/territorial electronic health record infrastructures regarding the functionality required by PPMS in order for pharmacists and pharmacy technicians to comply with their respective standards of practice.

Pharmacy regulatory authorities recognize that public safety also requires that measures be taken to prevent prescription fraud involving electronic prescriptions (e-prescriptions) and that these measures must be at least as robust as those that currently deter and detect fraud with paper prescriptions. Electronic prescribing (e-prescribing) allows prescribers to order and send prescriptions electronically so that a patient's pharmacist of choice can immediately access them. Some of the benefits attributed to e-prescribing depend critically upon ensuring the authenticity of e-prescriptions and securing their transmission from prescriber to dispenser.

The proposed 35 requirements addressing technical, functional and administrative requirements of PPMS are listed in Section 3. They cover the need for unique patient identifiers and unified patient records, the accurate identification of prescribers and system users, the restriction of access to patient data, acceptable uses of PPMS, user access control and logout of users, and termination of access privileges. They also address patient choice, patient consent restrictions, comprehensive medication profiles and clinical records and the sharing of those records, tracking patient progress, and lab test ordering by pharmacists. They address e-prescription authenticity and authoritative versions of e-prescriptions, prescription indications, and the accountability of pharmacists as they prescribe and dispense. They address PPMS capabilities including report generation, record integrity, secure transmission, secure messaging, secure data storage, and audit logging—including auditable events and the audit data recorded. The requirements also address storage of data outside of Canada, remote access, maintaining the availability of data, information management arrangements, confidentiality agreements for IT service support, PPMS privacy impact assessments, PPMS threat/risk assessments, training materials and documentation, and the responsibility of pharmacy licensees regarding training. Together, the requirements, when met, will ensure that PPMS are designed and used in ways that ensure the safety and efficacy of e-prescriptions and related electronic pharmacy records.

[1] Available at: http://napra.ca/Content_Files/Files/Model_Standards_of_Prac_for_Cdn_Pharm_March09_Final_b.pdf

[2] Canada Health Infoway, Canadian Electronic Drug Messaging (CeRx). Available at http://www.infoway.ca/

Table of Contents

1. Introduction

The information management systems used by pharmacy professionals (referred to in this document as pharmacy practice management systems or PPMS) must support the delivery of patient care, including the dispensing of drugs in accordance with federal/provincial/territorial regulations and standards. System ability to record, display, store, and exchange patient-specific information in a manner that optimizes workflow within pharmacy teams is critical, as is the ability to exchange information with other systems such as provincial health record systems. Effective systems should be integrated and interoperable. Systems must be developed using nationally recognized data and technical standards to facilitate both information exchange with external systems such as federal/provincial/territorial electronic health records, and processes such as electronic prescribing. They must be designed to support the privacy and security of personal health information[3] recorded and stored within, and transmitted to and from the systems.

Historically, PPMS have been developed to support dispensing and billing processes by vendors who interpreted practice requirements through consultation with customers. Despite the advent of the HL7 v3 pan-Canadian Messaging Standards[4], a common national direction has never been provided by pharmacy regulatory authorities to ensure that PPMS are able to support pharmacists and pharmacy technicians to effectively and efficiently fulfill their professional responsibilities; responsibilities which go beyond dispensing and which continue to evolve.

Provincial and territorial legislation authorize provincial/territorial pharmacy regulatory authorities to develop and enforce standards for pharmacists' practice and, in most jurisdictions, standards for the operation of pharmacies. Pharmacy practice management systems are a critical part of the infrastructure needed for effective compliance with these standards.

The National Association of Pharmacy Regulatory Authorities (NAPRA) is an association of the provincial and territorial organizations responsible for the governance of pharmacists and pharmacies. NAPRA provides a forum through which these provincial and territorial authorities cooperate in developing standards and programs that can be applied commonly across Canada (i.e., the *Model Standards of Practice for Canadian Pharmacists*). The Council of Pharmacy Registrars of Canada (CPRC) functions as an advisory committee of NAPRA, and includes the Registrars from each jurisdiction who are responsible for administering the practice of pharmacy and the operation of pharmacies.

[3] The term "personal health information" is defined in provincial personal health information legislation. The majority of Canadian provinces now have such legislation and there are other provinces and territories that, at the time of this writing, have draft legislation in progress or laws awaiting proclamation. While there are variations in the legal definitions, there are also many common understandings among Canada's Ministries and Departments of Health about what constitutes personal health information and what needs to be done to protect it. See for example: Canada Health Infoway, *Privacy and EHR Information Flows in Canada: Common Understandings of the Pan-Canadian Health Information Privacy Group*, July 31, 2012. Available at: https://www.infoway-inforoute.ca/index.php/resources/reports/privacy/doc_download/626-privacy-and-ehr-information-flows-in-canada-version-2-0

[4] For a description of these standards, see https://www.infoway-inforoute.ca/index.php/programs-services/standards-collaborative/pan-canadian-standards

A working group formed from among the Registrars and subject matter specialists from other pharmacy regulatory authorities developed requirements for pharmacy practice management systems used by pharmacy personnel across Canada: these requirements were presented to the Board of NAPRA and approved in principle. The "Model Standards of Practice" developed by NAPRA[5] and the pan-Canadian Drug Messaging Standard (CeRx and MR2009)[6] developed by Canada Health Infoway have informed the working group's discussions.

The purpose of these requirements is to instruct pharmacists, pharmacy managers, pharmacy owners, pharmacy practice management system vendors, and developers of federal/provincial/territorial electronic health records about the minimum functionality required by systems used in pharmacy practice in order for pharmacists and pharmacy technicians to comply with their respective standards of practice. The requirements do not contemplate inventory control, business management, or other functions that can optimize practices but have not been identified as requirements in the standards of practice.

The requirements are intended to direct the development and deployment of information management systems that enable patient care services within pharmacy practice and as such should be read by anyone involved in the acquisition or use of PPMS.

None of these requirements are intended to either repeat or replace the provisions of jurisdictional privacy and health information legislation and guidelines. Rather, they complement, and in some cases augment, existing provisions in law for protecting patient privacy and preserving the confidentiality and integrity of personal health information.

The requirements described herein should be considered minimum requirements for a PPMS: vendor software (alone or in combination with other software, systems, and services) must meet all the requirements listed below and perform all the mandatory functions described in this document before such software can be considered compliant with, and supportive of, NAPRA standards of professional practice and hence suitable for deployment.

It is not anticipated that provincial or territorial pharmacy regulatory authorities will be involved in the process of conformance testing of software. Some national organizations, such as Canada Health Infoway, currently provide pre-implementation certification testing for some aspects of electronic health record (EHR) and electronic medical record (EMR) software (e.g., EMR systems, consumer health applications, diagnostic imaging systems, and most importantly from the perspective of this report, drug information systems[7]). As well, some jurisdictions provide province-wide certification services (e.g., eHealth Ontario sets criteria for EMR certification testing and the testing is then carried out by OntarioMD[8]).

---

[5] NAPRA, *Model Standards of Practice for Canadian Pharmacists*, March 2009. Available at: http://napra.ca/Content_Files/Files/Model_Standards_of_Prac_for_Cdn_Pharm_March09_Final_b.pdf

[6] Canada Health Infoway, *Canadian Electronic Drug Messaging (CeRx)*. Available at: http://www.infoway.ca/

[7] For a description of certification services provided by Canada Health Infoway, see https://www.infoway-inforoute.ca/index.php/programs-services/certification-services

[8] For a description of certification services provided by OntarioMD, see https://www.ontariomd.ca/portal/server.pt/community/emr_offerings/offering_details/

2. Background

Pharmacy practice is evolving to include longitudinal care, with an increasing emphasis on patient-focused care, as compared to being primarily product-focused (i.e., drug distribution). Care is not based on a single transaction or episode, but rather includes multiple interactions with a patient over longer periods of time. Each time a patient accesses pharmacist care, an assessment of the individual and previous health records is required. Pharmacists across Canada are increasingly being empowered with new authorities to order laboratory tests, and to prescribe and administer drugs by injection; thereby enabling them to not just identify drug related problems, but rather to resolve them, and respond immediately to patient needs. Correspondingly, patient and third-party expectations of pharmacists are increasing. Therefore, integration of PPMS to other clinical systems or repositories (e.g., a provincial drug information system [DIS] or EHR) is essential.

An increasing number of jurisdictions in Canada are recognizing and regulating pharmacy technicians to enable pharmacists to focus on patient care roles. Generally, pharmacy technicians are authorized to compound and dispense prescription drugs, subject to a pharmacist determining that the therapy is appropriate.

Some jurisdictions are developing integrated electronic health records to improve care. By capturing patient care events and then storing them centrally (i.e. prescribing records, dispensing records, laboratory results), comprehensive patient care information is made available to an increased number of health professionals, facilitating improved decision-making at multiple points of care. New information technology (IT) enabled communication processes such as e-prescribing are also emerging to improve communication between health professionals.

Electronic prescribing (e-prescribing) allows prescribers to order and send prescriptions electronically so that a patient's pharmacist of choice can immediately access them. Some of the benefits attributed to e-prescribing depend critically upon ensuring the authenticity of e-prescriptions and securing their transmission from prescriber to dispenser. For example, Canada Health Infoway maintains that accessing prescriptions electronically increases the productivity of health professionals and helps keep patients safer by reducing medication errors[9] (although other evidence[10] has indicated that e-prescribing does not increase or reduce prescription errors, but rather changes the types of errors). Public safety also requires that measures be taken to prevent prescription fraud using e-prescriptions and that these measures need to be at least as robust as those that currently deter and detect fraud with paper prescriptions. By signing a prescription, a health care professional assumes accountability that the medication is both indicated and safe for the patient. A prescriber's signature on a paper prescription can be directly examined by a pharmacist and in many cases compared against previous prescriptions from the same prescriber. How can pharmacists be assured that an e-prescription is not fabricated or that a genuine e-prescription has not subsequently been fraudulently altered? Under what circumstances, if any, should a pharmacy professional call into question the authenticity of an e-prescription?

Traditional information systems used in pharmacies have evolved to accommodate business processes associated with the activity of dispensing, but are not effective in enabling and facilitating the recording, storage, and exchange of information used by pharmacy professionals in emerging patient care roles. Pharmacy regulatory authorities have a responsibility to communicate minimum requirements of systems used by pharmacists and pharmacy technicians in their delivery of quality care and services.

---

[9] Canada Health Infoway, *Health Care Providers Form Working Group to Maximize Value of e-Prescribing,* April 21, 2011. Available at: https://www.infoway-inforoute.ca/lang-en/about-infoway/news/news-releases/714-health-care-providers-form-working-group-to-maximize-value-of-e-prescribing

[10] Nanji KC, Rothschild JM, Salzberg C, et al. *Errors associated with outpatient computerized prescribing systems*; J Am Med Inform Assoc (2011). doi:10.1136/amiajnl-2011-000205

3. Requirements

To address the issues above, the CPRC proposed the following requirements to NAPRA's Board of Directors. Some of these requirements address technical requirements of PPMS; for example, the need for secure transmission of data. Some address functional requirements of PPMS; for example, the capability to produce reports on drug utilization. Some address administrative requirements (e.g., the need to limit access to personal information). Together, the requirements, when met, ensure that PPMS are designed and used in ways that ensure the safety and efficacy of e-prescriptions and related electronic pharmacy records.

All these requirements have been carefully reviewed to ensure their applicability to both community-based pharmacies and to hospital pharmacies.

Requirement 1: Unique Patient Record

Every PPMS must provide authorized users with the capability to create, access, and update a unique patient record such that:

a) each patient has a unique patient identifier within the PPMS;

b) patient identification functions provided by the PPMS support the identifiers, search tools and record management functions provided by applicable jurisdictional EHR or client registries, including the ability to add and update patient records where available;

c) each patient record contains essential patient demographics needed to confirm the patient's identity (including, names(s), address, gender, and date of birth) and communicate effectively with the patient (e.g., language preference); and

d) each patient record contains essential personal health information, including drug allergies or intolerances and medical history relevant to pharmacy practice.

Rationale

It is of the essence of electronic health records that all relevant clinical information for a patient be readily available. This includes ensuring that important patient data is not broken into disparate and disconnected records (i.e., one patient, many records). Patient safety also requires that all the information in a patient's record pertains to that patient and does not include information from unrelated patient records (i.e., one record, multiple patients).

[Note: Patient identification functions provided by PPMS need to support the identifiers and search tools provided by jurisdictional patient registries. Both Newfoundland and Labrador and British Columbia already support the ability of pharmacists to add new patients to the provincial client registry if they are not already present.]

See also Requirement 10: Comprehensiveness of Clinical Records

Requirement 2: User Identification

Every PPMS must clearly identify each user of the PPMS and the user's unique identification (ID).

[Note: this implies that all pharmacy staff members, including students, assistants, etc., require a unique account and cannot log in under the account of another pharmacy professional, even though the user may be performing services under the authority of that pharmacy professional.]

Rationale

Every user of a PPMS needs to be authenticated prior to accessing the PPMS and the confidential data and services that it contains. Effective user authentication in turn requires that each prospective user be registered and given a unique user ID, password, etc. If individual pharmacy professionals are not logged into the system as authenticated, authorized users, then unauthorized access cannot be prevented. Effective user identity management includes determining, as a matter of pharmacy practice, how unauthorized individuals are prevented from becoming users of the system and how formerly authorized users can have their privileges revoked.

[Note: As it is not the intention of this document to state general requirements that would apply to any well-constructed computer system, specific requirements for authentication techniques such as passwords are not stated. Authentication methods are an essential component of access control and their use is all but ubiquitous in computer software applications, whether they be in healthcare, or in other industrial sectors such as banking, manufacturing, or retail. Moreover, PPMS vendors are free to construct systems with robust authentication technologies that do not specifically involve passwords (e.g., physical tokens, biometrics, etc.). Password requirements have therefore not been addressed.]

Requirement 3: Access Control

Every PPMS must support role-based access control by assigning users to roles based upon their job responsibilities, and assigning roles to access privileges based upon the information access needs of the users carrying out those roles.

Rationale

Role-based access control allows different users to have different levels of access depending on their job functions. For example, certain users can be authorized to view prescriptions in the PPMS but not to alter them; or to view dispensing records but not to "sign" a dispensing record as having been dispensed. By mapping such access privileges to a small set of work-related roles, and then relegating users to those roles, the task of administering user privileges is considerably simplified. It also prevents security mistakes that might otherwise arise if each type of access or service had to be directly mapped to each and every user in a complex customized assignment.

Some jurisdictions have created guidelines for access control in healthcare. For example, British Columbia's guidelines for PharmaNet can be found at http://www.health.gov.bc.ca/access/pdf/catalogu/tech/ppscs5.pdf

[Note: while patients have a right to access their personal health records, it is not contemplated that patients be given direct access to a PPMS. Rather, a pharmacy professional accessing a PPMS would provide information to a patient, ensuring that the information provided was in an understandable form and given an appropriate explanatory context.]

[Note: The ability to edit or revise role definitions (i.e., which roles have which access privileges) is itself a role that must be carefully assigned. Determining which roles have which access privileges, as well as who administers such roles, involves policy decisions that lie outside the scope of this document.]

Requirement 4: Acceptable Use of PPMS

Prior to granting access to a PPMS system, the pharmacy licensee must obtain a signed user agreement from each prospective user that clearly indicates their roles and responsibilities when using the system, including their obligations with respect to the confidentiality of patient information.

Rationale

Acceptable use agreements between pharmacy licensees and users of the pharmacy's PPMS ensure that patient information is fully protected by each user and provide a legal redress should a user fail to uphold his or her contractual obligations with respect to maintaining this confidentiality.

Requirement 5: Logging Out Inactive Users

Every PPMS must automatically log out inactive users after a configurable period of time.

Rationale

In order for the audit function of a PPMS to function as designed, inactive users must be logged out, lest another user take over an inactive session and continue it with the result that the second user's actions are recorded as if those actions had been taken by the first user. Users who are inactive after a period of time therefore need to be automatically logged out. This time period should be configurable to best meet the needs of the pharmacy professionals and their workflow.

Requirement 6: Termination/Suspension of Access Privileges

Each pharmacy licensee must promptly terminate or suspend access privileges of each user of a PPMS upon termination or suspension of the user's employment and every PPMS must support termination or suspension of user accounts.

Rationale

Former employees who retain access privileges beyond their term of employment represent a potential risk to the confidentiality of patient information. Significant breaches of patient confidentiality have been caused by disgruntled former employees whose access to health information systems was not terminated in a timely manner.

Requirement 7: Patient Choice

A PPMS must not compromise the patient's choice of pharmacy or healthcare provider.

[Note: This requirement is not intended to suggest that an inpatient of a hospital can choose to receive medication dispensed by a different hospital pharmacy of their choosing.]

Rationale

The integrity of patient choice is one of the five principals espoused by NAPRA's Report On The Transfer Of Authority To Fill Prescriptions By Electronic Transmission[11].

Requirement 8: Patient Consent Restrictions

Every PPMS must:

a) access a patient's informational consent or disclosure directives, including the withholding or revocation of consent to disclose information to third parties, where such directives are available to pharmacy professionals from applicable jurisdictional EHR or client repositories;

b) enable an authorized user to record a patient's informational consent or disclosure directives and then update jurisdictional EHR or client repositories records where jurisdictional DIS or EHR component allow such updates from a PPMS;

c) accomplish this in a way that allows each jurisdiction to comply with its own legal or policy requirements on consent;

d) restrict access to electronic pharmacy records based upon a patient's informational consent or disclosure directives in addition to the user's access role; and

e) enable an authorized user to obtain emergency access to patient records overriding previously recorded disclosure directives (where emergency medical care or other special situations permitted by law or policy necessitate) and then record in an audit log the invocation of such overriding access, along with a user-provided reason as to why the consent directive was overridden.

Rationale

Legal requirements for informational consent vary somewhat among provinces and territories. PPMS need controls that allow a patient to restrict access to his/her prescriptions and dispensing records, as well as records of interventions, follow-ups, and other records locally stored in the pharmacy. Where such consent restrictions can be overridden in emergency situations, the act of doing so needs to be auditable in order to ensure that the patient wishes expressed in the consent restrictions are fully respected.

Requirement 9: Comprehensive Medication Profile

Every PPMS must provide authorized users with the capability to create, access, and update a comprehensive patient-specific medication profile. Examples include the dispensing of prescription and non-prescription drugs, medical devices, and other items of clinical significance.

Rationale

Whether or not a PPMS is interfaced to a jurisdictional DIS, it needs to be able to record a patient-specific medication profile for all prescriptions dispensed in the pharmacy as well as non-prescriptions and medical devices as appropriate.

[11] "Patient choice must be protected; that is, the patient must determine the practitioner to receive the prescription authority". NAPRA, *Report on the Transfer of Authority to Fill Prescriptions by Electronic Transmission*, 1998. Available at http://www.napra.ca/Content_Files/Files/electronic.pdf

Requirement 10: Comprehensiveness of Clinical Records

Every PPMS must provide authorized users with the capability to create, access, and update records of assessment, care planning, interventions (e.g., dispensing, prescribing, consultations, injections, lifestyle advice, referrals), and monitoring conducted by pharmacy professionals; including observed outcomes, assessment of patient progress and patient adherence to an established care plan, and all data specified in provincial/territorial pharmacy standards of practice. This functionality must provide users with the ability to report on various aspects of these records.

Rationale

The evolution of PPMS has not kept pace with the evolution of pharmacy practice which continues its increasing emphasis on patient-focused care versus the product-focused provision of service (i.e., drug distribution). Pharmacy records are more than a collection of prescriptions dispensed. Records also include all information used in clinical judgement and decision making and all activities associated with provision of care, including advice and clinical outcomes.

As traditional paper records are replaced by electronic equivalents, vendors will need to ensure that PPMS are capable of recording the full spectrum of patient information that pharmacy professionals need to assist them in treatment planning and the provision of patient-centric care as well as to better prepare for future integration with comprehensive EHR systems.

Pharmacy practice continues its development towards longitudinal care. Care is not based on a single transaction or episode, but rather includes multiple interactions with a patient over extended periods of time. Each time a patient accesses pharmacist care, an assessment of the individual and their history contained in previous records is required. At the time of each assessment, patient progress should be recorded in the Electronic Pharmacy Record (EPhR), including but not limited to compliance with the care plan, changes in health status, adverse events, and clinical indicators being monitored (e.g. HbA1c, BP, Wt.) The PPMS needs the capability to record decisions/interventions, including reasons/goals that the pharmacist makes in response to the assessment. The EPhR should evolve chronologically with each pharmacist/patient interaction.

[Note: As with other aspects of the PPMS, these tools need not be embedded in a single, monolithic PPMS software program. The functionality of these management tools may be provided by a PPMS that combines software packages, tools and IT services into a coherent system.]

Requirement 11: Sharing Clinical Records

Every PPMS must provide authorized users with the capability to:

a) access, for a given patient, all patient information available to pharmacy professionals from jurisdictional DIS and EHR repositories, and

b) update jurisdictional DIS records and/or EHR records of assessment, care planning, interventions, and monitoring conducted by pharmacy professionals, where jurisdictional DIS or other EHR component allow such updates from PPMS.

[Note: It is assumed that records accessed from a jurisdictional DIS or EHR repository will be available when needed, and that there is therefore no need to locally store in the PPMS medication profiles accessed from an EHR repository or DIS. This in turn assumes that the EHR/DIS has the same audit facilities described in Requirement 30 and that such audit information will be available to pharmacy regulatory authorities.]

Rationale

PPMS need to effectively allow access by pharmacy professionals to data from jurisdictional EHRs and DIS, including medication profiles. Just as importantly, PPMS need to update DIS data when the PPMS records information entered by pharmacy professionals is also recorded in the DIS. Only by doing so is it possible to fully maintain the integrity of the DIS, and ultimately each patient's EHR. While not every jurisdictional DIS or EHR will initially permit such updates, PPMS need to support whatever update capabilities exist.

Requirement 12: Lab Tests

Every PPMS must provide authorized users with the capability to:

a) access lab tests results in those jurisdictions where results can be accessed electronically;

b) order lab tests in those jurisdictions where pharmacists can electronically order such tests; and

c) obtain reports, in those jurisdictions where pharmacists can electronically order lab tests, of all tests ordered by a pharmacist where a result has not received by the pharmacist's PPMS, and of all test results received by a pharmacist's PPMS but not yet viewed by the pharmacist.

Rationale

The latency of results not received or reviewed in a timely manner could adversely affect patient safety. Pharmacists therefore need to track outstanding tests. Similarly, they need to be able to easily review test results received but not yet viewed in order to deal effectively with urgent or time-critical results.

[Note: As with other aspects of the PPMS, these facilities need not be embedded in a single, monolithic PPMS software program. The functionality of these management tools may be provided by a PPMS that combines software packages, tools and IT services into a coherent system.]

Requirement 13: Patient Identification on e-Prescriptions

Every PPMS must, for each e-prescription, clearly identify the patient and the patient's ID as found in a jurisdictional client registry, where such a registry exists.

[Note: This implies that, where a jurisdictional client registry exists, no e-prescription can be created for a patient who is not in the registry. Some client registries will allow the pharmacist to create a new patient record (the client registries of both British Columbia and Newfoundland and Labrador support this). In those jurisdictions that do not support this capability, paper or verbal prescriptions will need to be issued, as appropriate for patients not in the registry. See also Requirement 1.]

Rationale

No patient safety issue is perhaps more important than the accurate identification of the patient. Patient identifiers are essential information for pharmacists in ensuring that the right information has been entered into the right patient record. These patient identifiers are also used to link records to jurisdictional EHR systems, to EMR systems in medical practices, and to other repositories of patient information.

Requirement 14: Prescriber Identification

Every PPMS must, for each e-prescription, clearly identify the prescriber and the prescriber's ID, as found in a jurisdictional provider registry (where such a provider registry exists in the jurisdiction) and be capable, at the user's request, of displaying information linked to the prescriber from this jurisdictional provider registry.

[Note: this implies that no e-prescription can be created by a prescriber who does not have a registration record in a jurisdictional provider registry.]

Rationale

The rationale for this requirement is twofold. Accurate prescriber identification is essential for ensuring that pharmacy professionals can contact the prescriber if additional information is needed or if contraindications are discovered that impact patient safety. As well, by restricting e-prescriptions to those prescribers who are in a jurisdictional provider registry, pharmacy professionals gain important assurances about the authenticity of each e-prescription and the authorization of each prescriber to write such a prescription.

Requirement 15: Prescriber E-Prescription Authenticity

Every PPMS must:

a) receive and record evidence that the prescriber has authorized the prescription by electronic means [deliberate act of signing];

b) accept only e-prescriptions that are uniquely identified [e-prescription uniqueness]; and

c) use technical means to ensure that all e-prescriptions are received from a secure and trusted system [authentic sources for e-prescriptions].

Rationale

Pharmacy professionals need to know that an e-prescription has been "signed" by the prescriber; i.e., that it is the complete record of a deliberate act. To prevent duplicate dispensing, e-prescriptions need to be unique. Jurisdictional systems provide a unique number for each e-prescription and PPMS need to record and display such unique identifiers. Finally, a PPMS cannot accept e-prescriptions from an unknown source. Secure means of establishing the authenticity of the sending system need to be in place to prevent fraudulent prescriptions from being sent to pharmacies.

Requirement 16: Authoritative Version of E-Prescription

Every PPMS must provide unambiguous direction to pharmacy professionals as to whether an e-prescription constitutes the authoritative record of instructions to dispense or whether it is a copy (e.g., of a paper original) in order to ensure that the prescription is acted upon only once and to thereby prevent a patient from improperly filling it more than once.

Rationale

Paper will continue to be an established medium for prescriptions for many years to come and e-prescription systems will therefore need to co-exist with paper prescriptions for the foreseeable future. Pharmacy professionals will also need unambiguous direction as to whether a paper prescription (say, one printed out by an EMR) is an authentic original given to the patient in the absence of an e-prescription (and hence to be filled like any other paper prescription), or whether the paper is merely a receipt provided for the convenience of the patient who has been issued an e-prescription (and hence not to be filled in the absence of the e-prescription).

Requirement 17: Prescription Indications

Every PPMS must, for each prescription, provide authorized users with the capability to electronically access (in the case of e-prescriptions) or input (in the case of paper or verbal prescriptions) an indication or reason for use or therapeutic goal.

Rationale

To reduce prescription errors and make the most effective use of the medication profiles provided by federal/provincial/territorial DIS, pharmacy professionals need access to prescription indications or therapeutic goals, whenever such data have been provided by the prescriber.

To inform appropriate drug therapy, it is important that pharmacists and other members of patients' care teams understand why each medication is being used. Most medications are approved for more than one condition and appropriate dosing may vary depending on the condition or health status of the patient. Therefore, it is important for pharmacists to understand the reason that a drug is prescribed (e.g., to treat a rash) and whether there is a specific "approved indication" (e.g., to treat blood pressure) for which the drug is to be used. More specific information that identifies the therapeutic goal (e.g., to reduce blood pressure to 130/90) is even more beneficial.

Furthermore, evidence[12] has shown that e-prescribing does not increase or reduce prescription errors, but rather changes the types of errors. Selecting the wrong medication from a list is the most common error identified when employing computer-generated prescriptions. Inclusion of the reason for use, indication for use, or therapeutic goals as part of the e-prescription can enhance patient safety by making such errors apparent.

See also the note at the end of Requirement 12.

[12] Nanji KC, Rothschild JM, Salzberg C, et al. *Errors associated with outpatient computerized prescribing systems*; J Am Med Inform Assoc (2011). doi:10.1136/amiajnl-2011-000205

See also: Gaunt MJ. *Continued Efforts Needed to Design Safer e-Prescribing Systems*, Pharmacy Times, January 20111. Available at: http://www.pharmacytimes.com/publications/issue/2011/January2011/MedSafety-0111

See also: Redley B; Botti M. *Reported medication errors after introducing an electronic medication management system,* J Clin Nurs. 2013 Feb; 22(3-4):579-89. doi:10.1111/j.1365-2702.2012.04326.x.

Requirement 18: Accountability of Prescribing Pharmacist

Every PPMS must record evidence, by electronic means, that an identified pharmacist has signed each e-prescription generated via the PPMS in a deliberate and auditable act.

[Note: An order including multiple e-prescriptions may all be covered by a single deliberate and auditable act by the pharmacist prescriber.]

Rationale

In several Canadian jurisdictions, pharmacists can now prescribe drugs. To support the role of pharmacists as prescribers, PPMS need to have the same capabilities that EMR systems provide to physicians to accurately capture e-prescriptions. See also Requirement 15.

Requirement 19: Accountability of Dispensing Pharmacist

Every PPMS must record evidence, by electronic means, that an identified pharmacist has authorized the dispensing of each prescription and, where applicable, that one or more pharmacy technicians have completed the permitted functions.

Rationale

As paper prescriptions are displaced by e-prescriptions, pharmacists will need an electronic equivalent of signing a paper prescription when it is dispensed. Pharmacists are responsible for determining the appropriateness of each prescription prior to it being released to the patient. If performed by a pharmacy technician, accuracy of drug, dosage form and dose of final product is the responsibility of the dispensing pharmacy technician.

Requirement 20: Reports

Every PPMS must enable the pharmacy licensee to generate reports on the data fields stored in the pharmacy-managed (i.e., "local") PPMS.

These reports include, but are not limited to, patient-specific, prescriber-specific, drug-specific, and drug-class-specific analyses and also include reports that identify individual patients, as well as those that provide aggregate data only (and therefore do not contain patient-identifiable data).

Rationale

As provinces and territories direct increasing attention to effective drug utilization, patterns of narcotic prescribing, and drug recall, pharmacy professionals need flexible reporting functionality for generation of drug utilization reports. Ultimately, PPMS need to be able to report on any field of data recorded and break down data by patient, by prescriber, and even by drug or drug class.

[Note: when a report is generated that includes personally identifiable data, its generation is an auditable event as discussed below in Requirement 30.]

Requirement 21: Data Integrity

Every PPMS must provide authorized users with the capability to:

a) display any patient's pharmacy record(s) exactly as the record(s) existed electronically within the pharmacy at any prior date and time;[Note 2]

b) accurately display French language accented characters in text fields;

c) display the origin of any data received electronically;[Note 3]

d) display the date(s) and time(s) of any change(s) made to pharmacy records and the user(s) responsible for the changes; and

e) allow a reason for changes made to data to be entered by the user updating the record.

[Note 1: pharmacy practice management records include patient records as described in Requirement 1, medication profile records as described in Requirement 9, and clinical records as described in Requirement 10.]

[Note 2: Clause a) applies only to electronic patient pharmacy records as they exist on the date these requirements come into effect and going forward.]

[Note 3: Clause b) does not apply to historical records beyond established jurisdictional records retention requirements.]

Rationale

PPMS need to be capable of displaying the content of a prescription as it was received by the pharmacy and highlighting any changes made to the prescription during dispensing. Without such a capability, pharmacy regulatory authorities cannot readily determine the content of a prescription at the time it was dispensed, the information available to the pharmacist at the time of dispensing, and the precise nature of any changes made to the prescription (if any), prior to it being dispensed. This in turn impedes audits of pharmacy practices and the fair, efficient, and thorough investigation of patient complaints. This issue is especially problematic for e-prescriptions, as without the capabilities described in the requirements above, there would be no electronic equivalent to the written record of edits, corrections and amendments that can be found on paper prescriptions.

Requirement 22: Safety and Quality

Every PPMS must provide authorized users with the capability to:

a) create, access, and update records of reported adverse drug events, medication errors, incidents, close-calls and unsafe practices;

b) generate reports necessary for appropriate management of such events and continued quality improvement; and

c) generate reports required to comply with federal/provincial/territorial legislation on adverse drug event reporting.

Rationale

NAPRA Standards of Practice require that pharmacists respond to safety risks. Specifically, the standard addresses pharmacists' obligation to manage errors, incidents and unsafe practices as well as develop and implement policies and procedures that minimize errors, incidents and unsafe practices. The NAPRA standard also addresses pharmacists' obligation to report adverse events. PPMS functionality must facilitate proper recording, reporting, monitoring and evaluation of these events. Additionally, post-marketing surveillance and pharmacovigilance are increasingly important to Canada's health system. PPMS functionality needs to facilitate reporting to add to this body of knowledge.

Requirement 23: Information Management Agreements

Each pharmacy licensee must enter into an information management agreement with any third party to whom information is transmitted for the purpose of managing data on the licensee's behalf. In particular, prior to disclosing electronic pharmacy records or granting access to a PPMS, a pharmacy licensee must be satisfied that third-party information managers ensure the confidentiality and security of all identifiable personal health information collected, used, or retained.

[Note: As a matter of routine practice, pharmacies share billing data with Ministries and Departments of Health. These data disclosures are enabled by law and do not require information management agreements but may require jurisdiction-specific information sharing agreements. This is also true of legally mandated disclosures of clinical data to Ministries or Departments of Health or to crown agencies empowered to run jurisdictional repositories such as provider registries and DIS repositories. Such legally mandated disclosures do not require information management agreements.]

Rationale

The question of whether help-desk personnel or other vendor support personnel can be exposed to personal health information from a PPMS system is an especially important one. What protections—administrative, contractual or technical—protect patient privacy and prevent disclosure of personal health information from the PPMS?

Confidentiality agreements between pharmacy licensees and third parties who obtain, store or process information on behalf of the pharmacy ensure that the confidentiality of patient information is fully protected by the third party and provide legal redress should such a third party fail to uphold its contractual obligations.

Examples of such agreements include information management agreements between licensees and corporate pharmacy head offices, and providers of services that analyse patient identifiable data to produce reports on behalf of the pharmacy licensee.

Requirement 24: Confidentiality Agreements for Service Support

Each pharmacy licensee must enter into a confidentiality agreement with any third party to whom information is transmitted for the purpose of providing information technology services on the licensee's behalf. In particular, prior to disclosing electronic pharmacy records or granting access to a PPMS, a pharmacy licensee must be satisfied that PPMS vendors, IT service vendors, vendor support staff, and help desk personnel ensure the confidentiality and security of all identifiable personal health information collected, processed or retained.

Rationale

The question of whether help-desk personnel or other vendor support personnel can be exposed to personal health information from a PPMS system is an especially important one. What protections—administrative, contractual or technical—protect patient privacy and prevent disclosure of personal health information from the PPMS?

Confidentiality agreements between pharmacy licensees and third parties who obtain, store or process information on behalf of the pharmacy ensure that the confidentiality of patient information is fully protected by the third party and provide legal redress should such a third party fail to uphold its contractual obligations.

Requirement 25: Secure Transmission

Every PPMS that electronically receives or transmits personal health information, including electronic pharmacy records, by using a publicly accessible network, including the Internet, must do so by means of a securely encrypted transmission that cannot feasibly be intercepted or altered by an unauthorized third party, either at the time of transmission or in the foreseeable future.

[Note: A PPMS in a hospital may be attached to a secure private network within the facility. External transmission to/from a jurisdictional DIS or EHR, however, must meet the requirement that the transmission be securely encrypted, as must any transmission of personal health information across the Internet to a community pharmacy, physician practice or clinic.]

Rationale

Without the application of information security technology to ensure that all such transmissions are secured, e-prescriptions (along with other transmissions containing personal health information) may be subject to serious breaches of confidentiality or integrity. Any such breach has the potential to seriously erode trust in e-prescribing (and electronic health records in general).

Some jurisdictions have guidelines available on the security of health information. For example, the Ontario Information and Privacy Commission has produced guidelines on requirements for encryption for personal health information.[13]

Requirement 26: Secure Messaging With Other Healthcare Providers

Where messaging to other healthcare providers is enabled (e.g., via e-mail), every PPMS must ensure that such messages are securely encrypted such that they cannot feasibly be intercepted or altered by an unauthorized third party, either at the time the message was sent or while awaiting delivery.

[Note: A PPMS in a hospital may be attached to a secure private network within the facility. Messaging to/from a healthcare provider outside the facility (e.g., to a community pharmacy, physician practice, or clinic) must meet the requirement that the message be securely encrypted whenever the message contains personal health information. This includes messaging by e-mail.]

[13] Available at http://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=969 Note: in the interest of full disclosure, one of the authors of this report (Ross Fraser) is also a co-author of the guidelines references.

Rationale

The Internet is not a suitable medium for the transmission of unencrypted personal information. Without properly implemented security techniques such as encryption, the confidentiality of patient information will be unacceptably at risk.

In future, if messaging is supported directly to patients, the same provisions will apply.

Requirement 27: Secure Storage

Every PPMS must securely store and manage all electronic pharmacy records and audit log records, so that they cannot be accessed or altered by an unauthorized third party at any time during their life cycle or archival storage.

[Note: Secure storage is accomplished either through physical security of the storage medium (e.g., a locked data centre) or by means of encrypting the data stored.]

Rationale

Serious breaches of patient confidentiality have occurred in Canada when identifiable patient information was stored on unsecured computers or storage media. While risks to confidentiality also exist with paper records, it is in the nature of computerized records management that when such breaches occur, they involve thousands and sometimes tens of thousands of records. Patient trust in e-prescribing as a safe, confidential, and effective replacement for paper prescriptions will depend upon the secure storage and management of electronic patient records.

Patient information stored in a PPMS will need to be protected from unauthorized access or disclosure through equipment theft or loss of portable media.

Requirement 28: Storage of Electronic Pharmacy Records Outside of Canada

PPMS must not store any unencrypted electronic pharmacy records or audit log records outside of a Canadian jurisdiction.

Rationale

The storage of unencrypted electronic pharmacy records or audit log records outside of Canada may hinder the application of privacy protections otherwise available to patients under Canadian law and can complicate issues of measuring third-party compliance with contractual provisions to protect patient confidentiality.

It is important to note that strongly encrypted data is secure no matter where it is stored. Conversely, unencrypted data is subject to theft of its storage medium and there have been numerous incidents in Canada of personal health data being lost or stolen because they were stored portable computers or media in unencrypted form.

Requirement 29: Remote Access

Pharmacy professionals must only access electronic pharmacy records or use PPMS services remotely if such access uses secure transmission (see Requirement 25), incorporates access control (see Requirement 3), and does not store unencrypted personal health information (see Requirement 27) on the user's remote computer.

Rationale

The flexibility provided by working outside of a dispensary cannot come at the expense of patient confidentiality and data security. Remote access can represent a serious threat to patient privacy if it leaves unencrypted copies of patient records on laptops, mobile devices, or shared desktop computers. Care needs to be taken by the architects of portal applications and pharmacy viewers to ensure that remote access to a patient's records leaves no locally stored data behind in unencrypted form that could later be accessed by an unauthorized third party.

Requirement 30: Auditable Events and Audit Information Recorded

Every PPMS must:

a) record events related to system use (i.e., user login and logout, session timeout, data backup and restoration), processing of electronic pharmacy records (i.e., record creation, transmission, access, modification, and deletion), disclosure of electronic pharmacy records (i.e., import, export, transfer, printing, or other disclosure), overriding of consent directives (where permitted), and electronic signing of e-prescriptions or dispensing records by a pharmacy professional;

b) for each auditable event recorded in the audit log, keep an audit record of the time and date of the event, the identity of the user, the identity of the patient, the type of event, and (where supplied by a user), the reason given for the modification of a data field (see Requirement 21 d);

c) protect the audit log files to prevent any alteration or unauthorized access;

d) restrict access to the audit log and record such access as an auditable event, and provide the tools to extract audit information from audit records and interrogate the audit log to:

i) identify all users who have accessed or modified a given patient's records over a given period of time, or

ii) identify the actions of a given user (including all access to any patient records) over a given period of time.

e) retain audit log information for as long the underlying e-prescription and dispensing records are retained; and

provide reporting capabilities that allow the audit trail to be displayed.

Rationale

Pharmacy regulatory authorities need to have access to audit information such as what prescriptions were received by the pharmacy, when the prescriptions were received, transferred, or dispensed, the identity of the patients, which users have accessed specific records, and when, and the identity of the responsible parties (the prescriber and the dispenser). This is especially true of modifications or annotations to prescription information or medical history, as clinical decisions are influenced by such data. Privacy legislation mandates that even demographic information may be considered personal health information when presented in context with clinical data and patients may have the right to know who has accessed such data (e.g., a patient address).

Pharmacy regulatory authorities also need to have adequate information about the safeguards in place and adequate data in the audit logs to ensure that pharmacy records under audit have not been tampered with. As well, audit logging requirements are included in some jurisdictional health information privacy legislation; e.g., the Alberta Health Information Act (RSA 2000, c H-5, section 56.6(1)).

Requirement 31: Maintaining the Availability of Electronic Pharmacy Records

Every PPMS must support the generation of offsite backup copies of all data, security credentials, audit log files, and other data and files needed to return the PPMS to a fully operational and secure state. If the PPMS is available continuously, then the system must have the ability to run a backup concurrently with the operation of the system.

Rationale

Servers and storage media fail. Data that is not backed up is data at risk. As local servers are also subject to fires, floods, and other environmental failures, backed up data needs to be stored where it is protected from such disasters. As backup data from a PPMS will contain personal health information, the confidentiality and integrity of this backup information needs to be adequately protected. Such offsite backup is now considered standard practice.[14]

Information systems used in pharmacy must be resistant to failure and this extends beyond the mere availability of backups to a broad range of system reliability and availability requirements for such systems. While the robustness of integrated systems is a critical component of successful implementation, specific operational requirements for such systems are beyond the scope of this report.

Finally, when a pharmacy moves to a new software vendor or system, consideration needs to be given to how archival information will remain accessible. For example, an old system could partially be retained to allow retrieval of old records.

Requirement 32: PPMS Privacy Impact Assessment

Every PPMS must undergo a privacy impact assessment (PIA) that includes a data flow analysis and a legislative analysis pertinent to the province or territory where the system is being used.

[Note 1: A PIA for a PPMS may *not* necessarily need to be redone for each installation of the PPMS or even each installation in a new province or territory, although in the latter case, an existing PIA may need supplementary material to address specific issues arising from a jurisdiction's specific health information privacy legislation. A provincial or territorial regulatory authority may ask to review a PIA conducted in another jurisdiction and it reserves the right to require another PIA be conducted if it is deemed that the results presented in the reviewed PIA do not demonstrate compliance with the regulatory authority's particular requirements.]

[Note 2: A software vendor or application service provider cannot reasonably be expected to perform an impartial assessment on their own software products or services. However, an independent third-party (e.g., an information security consulting firm) may be contracted by a vendor or service provider to provide such an impartial assessment.]

[14] See for example ISO 27799.

Rationale

Privacy impact assessments are now routinely used in most federal/provincial/territorial jurisdictions to assess the potential impacts to patient privacy of health information systems. Vendors need to ensure that their PPMS meet legislative requirements of provincial/territorial personal health information protection laws. They also need to ensure that data flows (including transmission of data from the PPMS) do not compromise patient confidentiality. Pharmacy managers need to ensure that business practices and support processes are in place to ensure that patient privacy is maintained when a new PPMS is installed. A privacy impact assessment is an ideal tool for obtaining such assurances.

Several provincial privacy commissioners have set out guidelines for the conduct and content of PIAs, for example in Alberta: http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf and in Ontario: http://ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=574 While both guidelines contain some advice specific to their respective provinces, both also provide excellent general guidance applicable anywhere in Canada.

PIAs are also performed on jurisdictional DIS systems by provincial/territorial agencies charged with delivering such infrastructure. In several jurisdictions, such PIAs are reviewed by the jurisdictional privacy commission to ensure their comprehensiveness and integrity and to follow up on recommendations contained therein.

Requirement 33: PPMS Security Threats and Risks

Every PPMS must undergo a threat and risk assessment (TRA) and should be reassessed after significant changes to structure or functionality.

[Note 1: As with PIAs, a TRA for a PPMS does *not* need to be redone for each installation of the PPMS or even each installation in a new province or territory.]

[Note 2: As with PIAs, a software vendor or application service provider cannot reasonably be expected to perform an impartial assessment on their own software products or services. However, an independent third-party (e.g., an information security consulting firm) may be contracted by a vendor or service provider to provide an impartial TRA.

Rationale

Security-related threats and risks to health information systems are best assessed by means of a formal threat and risk assessment. For example, all Canada Health Infoway-funded EHR projects must undergo such threat and risk assessments.

In Canada, the federal Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP) have cooperated to provide harmonized standard guidelines for threat and risk assessments available at http://www.cse-cst.gc.ca/its-sti/publications/tra-emr/index-eng.html The guidelines are applicable anywhere in Canada and provide both excellent general guidance and specific, proven methodology.

Requirement 34: Training Materials and System Documentation

Every PPMS must have available up-to-date documentation that addresses system requirements and capacities, installation and testing, management and ongoing operation, known security issues, user identification, authentication, privilege management and access control, secure communications, audit, software change management, and data backup and restoration.

Rationale

PPMS vendors need to provide up-to-date training materials, courses, or other materials that promote the safe, secure, and privacy-protective use of their system. Users need these materials to ensure that they fully understand the system's features and use these features appropriately. Administrators need clear documentation on user management to ensure that access controls are properly administered and maintained. IT staff members need documentation for secure installation, operation, and ongoing upgrades of the system and to ensure effective disaster recovery and business continuity.

Requirement 35: Responsibility of the Licensee Regarding Training

Pharmacy licensees must ensure that all PPMS users have training that is adequate for fulfilling their professional responsibilities.

Rationale

PPMS can be powerful and effective tools that support and facilitate the work of pharmacy professionals, but only if such systems are properly used. It is the responsibility of each pharmacy licensee to ensure that all PPMS users have adequate training in all of the system functions to which they have access.

4. Interpretation

Readers should refer to the NAPRA *Model Standards of Practice for Canadian Pharmacists* for further insight on the fields and datasets that are required to support patient assessment, care-planning, interventions, and monitoring.

5. Effective Date

These requirements will come into effect January 1, 2016.

6. Future Opportunities and Challenges

A cumulative patient pharmacy record or cumulative patient pharmacy profile would make patient-related pharmacy information more readily accessible to pharmacists, in much the same way that the cumulative patient profile from an EMR does for physicians.[15] The cumulative patient pharmacy profile would incorporate components from a patient's cumulative patient profile which are relevant to pharmacy, such as relevant family history, medical history, lab values, etc., as well as pertinent information from the EPhR. Currently, there is no detailed definition of what information would be contained in a cumulative patient pharmacy profile. Establishing standards for what constitutes a comprehensive, complete, and current patient record will help to ensure patient record integrity and should be the next area to address in the future.

Therapeutic goal was discussed in Requirement 17: Prescription Indications. There is currently no support for specification of therapeutic goal in the pan-Canadian Drug Messaging Standard (CeRx and MR2009). The standard should be revised to incorporate this important data field. Consideration should be given by the Infoway Standards Collaborative as to whether a standardized set of values can be adopted, rather than a purely text-based field whose input values are entirely left to the discretion of the user.

Some aspects of data exchange between PPMS and jurisdictional EHR or DIS repositories lack detailed pan-Canadian standardization of a kind that would simplify for vendors the task of creating robust PPMS with the functionalities described in this document. Standardization efforts are ongoing (for example, within the Infoway Standards Collaborative) and such efforts need to be encouraged and supported with broad participation from vendors and jurisdictions.

The flow of e-prescriptions and DIS records across Canadian jurisdictional boundaries poses many challenges. Some jurisdictional DIS systems were not built with interoperability in mind: for example, both BC PharmaNet and the Manitoba Drug Program Information Network were fully operational years before Canada Health Infoway and its EHR-related activities came into existence. The data content of DIS repositories is not fully standardized by agreed upon pan-Canadian standards. Support for translation of prescriptions between English and French is also a non-trivial undertaking, but an important component of cross-jurisdictional interoperability in a bilingual country, as well as an important feature within bilingual jurisdictions or regions.

[15] Electronic Medical Record (EMR) systems provide physicians with a "cumulative patient profile," which separates pertinent information from the patient history from the continually updated information on short-term problems. The cumulative patient profile can avert repetitive history-taking and can make information more readily accessible to busy physicians.

Personal health records have been discussed in Canada for several years. Distinct from electronic health records, personal health records consist of information directly input by patients themselves or input at their request by their healthcare providers and then made directly accessible by the patients. Personal health records have purported benefits,[16] especially for patients with chronic conditions, but their future use in pharmacy remains unclear. Moreover, some highly publicised personal health record initiatives have since been abandoned (e.g., Google Health, announced in 2008 but cancelled in 2011 for lack of uptake). If a substantial number of Canadians adopt personal health record services in the future, the integration of pharmacy medication profiles with such services will need to be carefully examined.

Conformance testing and certification of software were briefly discussed in the Introduction. While Canada Health Infoway and some jurisdictions provide certification of certain aspects of some types of health software, it remains unclear how a jurisdictional pharmacy regulatory authority could be satisfied that a given vendor's PPMS offerings satisfy the requirements described in this document. Mutual endorsements of the requirements by both regulatory authorities and vendors are important steps toward a more formal process and valuable in their own right, as are statements of conformance made by vendors that can be taken at face value. In future, a more formal certification process may be desirable.

Finally, clinical decision support (e.g., drug-drug interactivity checking) has long been available to pharmacists by means of jurisdictional drug information systems such as BC PharmaNet. What is the role of PPMS in providing clinical decision support in the absence of a jurisdictional drug information system, or of augmenting jurisdictional clinical decision support where it is present? PPMS must evolve to integrate decision support tools that alert pharmacists to potential therapeutic, dosing, and safety considerations that are both drug and patient specific (e.g., age-related dosing adjustments or drug advisories from Health Canada). Display of this knowledge should be intuitive at the point of care. How this is best done requires further discussion and study in order to equip Canadian pharmacists from all jurisdictions with the decision support tools that would best serve their patients.

[16] Tang, Paul; Ash, Joan; Bates, David; Overhage, J.; Sands, Daniel (2006). "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption". JAMIA 13 (2): 121–126.

7. References

Canada Health Infoway. *Pan-Canadian Drug Messaging Standard (CeRx and MR2009)*. Available via: https://www.infoway-inforoute.ca/index.php/programs-services/standards-collaborative/pan-canadian-standards/drug-standard

Canada Health Infoway. *Certification Services*. Available at: https://www.infoway-inforoute.ca/index.php/programs-services/certification-services

Canada Health Infoway. *Electronic Health Record Blueprint*, version 2, 2006

Canada Health Infoway. *Health Care Providers Form Working Group to Maximize Value of e-Prescribing,* April 21, 2011. Available at: https://www.infoway-inforoute.ca/lang-en/about-infoway/news/news-releases/714-health-care-providers-form-working-group-to-maximize-value-of-e-prescribing

Canada Health Infoway. E-Prescribing Harmonization Project, *ePrescribing Reference Specification*

Canada Health Infoway. *Pan-Canadian Standards*. Available at: https://www.infoway-inforoute.ca/index.php/programs-services/standards-collaborative/pan-canadian-standards

Canada Health Infoway. *Privacy and EHR Information Flows in Canada: Common Understandings of the Pan-Canadian Health Information Privacy Group*, July 31, 2012. Available at: https://www.infoway-inforoute.ca/index.php/resources/reports/privacy/doc_download/626-privacy-and-ehr-information-flows-in-canada-version-2-0

Communications Security Establishment and the Royal Canadian Mounted Police. *Harmonized Threat and Risk Assessment (TRA) Methodology*, October 23, 2007. Available at: http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf

Gaunt MJ. *Continued Efforts Needed to Design Safer e-Prescribing Systems*, Pharmacy Times, January 2011. Available at: http://www.pharmacytimes.com/publications/issue/2011/January2011/MedSafety-0111

Information and Privacy Commissioner of Ontario. *Health-Care Requirements for Strong Encryption*, July 16, 2010. Available at http://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=969

Information and Privacy Commissioner of Ontario. *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, 2005. Available at: http://ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=574

International Organization for Standardization (ISO). *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture* (ISO 7498-2), 1989.

International Organization for Standardization (ISO). ISO 27799 Health *Informatics -- Information security management in health using ISO/IEC 27002, 2008.*

Nanji KC, Rothschild JM, Salzberg C, et al. *Errors associated with outpatient computerized prescribing systems*; J Am Med Inform Assoc (2011). doi:10.1136/amiajnl-2011-000205

National Association of Pharmacy Regulatory Authorities. *Model Standards of Practice for Canadian Pharmacists*, March 2009. Available at: http://napra.ca/Content_Files/Files/Model_Standards_of_Prac_for_Cdn_Pharm_March09_Final_b.pdf

National Association of Pharmacy Regulatory Authorities. *Report on the Transfer of Authority to Fill Prescriptions By Electronic Transmission*, 1998. Available at http://www.napra.ca/Content_Files/Files/electronic.pdf

Office of the Alberta Information and Privacy Commissioner. *Privacy Impact Assessment Requirements for Use With the Health Information* Act, 2009. Avaiable at http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf

OntarioMD. *OntarioMD Funding Eligible Offerings*. Available at https://www.ontariomd.ca/portal/server.pt/community/emr_offerings/offering_details/

PharmaNet. *Professional and Software Compliance Standards, Volume 5 – Security*, Version 3.2, April 2010 Available at http://www.health.gov.bc.ca/access/pdf/catalogu/tech/ppscs5.pdf

Redley B; Botti M. *Reported medication errors after introducing an electronic medication management system* J Clin Nurs. 2013 Feb; 22(3-4):579-89. doi:10.1111/j.1365-2702.2012.04326.x.

Tang, Paul; Ash, Joan; Bates, David; Overhage, J.; Sands, Daniel (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. J Am Med Inform Assoc 13 (2): 121–126. doi:10.1197/jamia.M2025

8. Terms and Definitions

Term	Definition	Reference
Circle of Care	The persons participating in - and the activities related - to the provision of health care to the individual who is the subject of the personal health information and includes necessarily incidental activities such as laboratory work and professional consultation.	Personal Health Information Act, SNL 2008, c P-7.01. Consolidated Statutes of Newfoundland and Labrador
Client Registry	A Client Registry or Enterprise Master Patient Index (EMPI) is a system which coordinates client identification across multiple systems namely by collecting and storing IDs and person-identifying demographic information from source system (track new persons, track changes to existing persons). These systems also take on several other tasks and responsibilities associated with client ID management. An electronic registry of demographic and administrative information related to individuals who have received health care in [a] province [or territory] that enables the accurate identification of individuals in the provincial [or territorial] EHR by linking person-specific information from separate clinical information systems to the correct individual.	Canada Health Infoway, *Electronic Health Record Blueprint*, version 2, 2006 Newfoundland and Labrador Centre for Health Information
Clinical decision support	Used when referring to a type of system that assists health care providers in making medical decisions. These types of systems typically require input of patient-specific clinical variables and as a result provide patient-specific recommendations.	Health Level Seven
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes.	International Organization for Standardization (ISO), *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture* (ISO 7498-2), 1989.

Term	Definition	Reference
Consent (withholding or withdrawal)	The act of an individual expressly stating that they do not consent to a particular activity. Withholding or withdrawing of consent typically occurs when an individual wishes to revoke his/her consent to make his/her records of personal health information available through an EHR. More specifically, withholding of consent occurs when an individual indicates that he/she does not want to consent to the sharing of his/her personal health information via the EHR prior to it initially being made available on the EHR. Withdrawing of consent occurs when an individual has either expressly provided consent or his/her consent has been implied for his/her personal health information to be shared via an EHR and then they revoke that consent at some later date. Note: in this document, the phrase "informational consent" is to specifically refer to consent to share or disclose information, in contradistinction to "consent to treatment" – the latter is outside the scope of this document.	Canada Health Infoway
Council of Pharmacy Registrars of Canada	A council consisting of federal, provincial and territorial registrars of pharmacists. See http://napra.ca/pages/About/CouncilofPharmacyRegistrarsofCanada.aspx	
CPRC	Council of Pharmacy Registrars of Canada	
DIS	See *Drug Information System*	
Drug Information System (DIS)	An EHR system and/or collection of services that offers real-time access to patient medication profiles, as well as comprehensive drug information and an interactive database to assist pharmacists and physicians in identifying potential adverse drug interactions and events. It is also the jurisdictional repository that receives and manages medication prescriptions and dispensation events.	Canada Health Infoway E-Prescribing Harmonization Project, *ePrescribing Reference Specification*
EHR	See *Electronic Health Record*	
Electronic Health Record (EHR)	An Electronic Health Record (EHR) provides each individual in Canada with a secure and private lifetime record of their key health history and care within the health system. The record is available electronically to authorized health care providers and the individual anywhere, anytime in support of high quality care.	Canada Health Infoway, *EHRS Blueprint Version 2*, 2006, page 326

Term	Definition	Reference
Electronic Medical Record (EMR)	A general term describing computer-based patient record systems. It is sometimes extended to include other functions like order entry for medications and tests, amongst other common functions.	Canada Health Infoway, Canadian Electronic Drug Messaging (CeRx)
Electronic Pharmacy Record (EPhR)	A general term describing computer-based patient records used in the practice of pharmacy. The EPhR is the record created in the PPMS including information about a patient, care decisions made by pharmacy professionals, and services provided by pharmacy professionals (record of care), as required by NAPRA standards of professional practice.	
Electronic prescribing	A means of streamlining the prescription process by enabling prescriptions to be created, signed and transmitted electronically. The secure electronic transmission from the authorized prescriber of a prescription to a patientss pharmacy of choice integrated with pharmacy software. The secure electronic creation and transmission of a prescription between an authorized prescriber and a patient's pharmacy of choice, using clinical Electronic Medical Record (EMR) and pharmacy management software.	Health Canada, Policy Statement on e-Prescribing National e-Pharmacy Task Force, *Recommendations for the Implementation of Electronic Prescriptions in Canada*, 2009 Canadian Medical Association and Canadian Pharmacists Association ePrescribing Working Group
EMPI	See *Enterprise Master Patient Index*	
EMR	See *Electronic Medical Record*	
Enterprise Master Patient Index (EMPI)	An Enterprise Master Patient Index (EMPI) or Client Registry is a system which coordinates client identification across multiple systems namely by collecting and storing IDs and person-identifying demographic information from source system (track new persons, track changes to existing persons). These systems also take on several other tasks and responsibilities associated with client ID management.	Canada Health Infoway, *Electronic Health Record Blueprint*, version 2, 2006

Term	Definition	Reference
EPhR	See *Electronic Pharmacy Record*	
E-prescription signing	Whatever is determined to be necessary to authenticate and validate the order in that pharmacists must have a high degree of certainty that the identified practitioner (in the electronic message) has ordered the prescription.	Health Canada, Policy Statement on e-Prescribing
Integrity (of data)	The property that data has not been altered or destroyed in an unauthorised manner.	International Organization for Standardization (ISO), *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture* (ISO 7498-2), 1989.
NAPRA	National Association of Pharmacy Regulatory Authorities	
Pharmacy licensee	Licensed clinical pharmacist that is granted a licence to operate a pharmacy. This person may also be referred to as the pharmacy manager.	Alberta College of Pharmacists
Pharmacy Practice Management System (PPMS)	An electronic system that supports the provision of pharmacy patient care as defined through NAPRA standards of professional practice. A PPMS facilitates the recording, use and disclosure of electronic pharmacy records and reporting on these records. Note: PPMS capabilities need not be embedded in a single, monolithic software program. PPMS functionality may be provided by a combination of software packages, tools and IT services that together function as a coherent system.	
Pharmacy professional	An individual registered with, and regulated by, a provincial or territorial pharmacy regulatory authority.	
PPMS	See *Pharmacy Practice Management System*	
Practice management system	Generic term used to reference a management system.	Canada Health Infoway, *Electronic Health Record Solution (EHRS) Blueprint,* version 2, 2006

Term	Definition	Reference
Provider registry	A system or a combination of systems where a health care provider's information (i.e. name, address, practice licences, etc.) is securely stored, maintained and made available to other systems and users. A provincial [or territorial] registry that provides unique IDs for all authorized health care providers and their locations. It includes other identifiers about a provider including licensing data, but only includes information that is already in the public domain.	Canada Health Infoway, *Electronic Health Record Blueprint*, version 2, 2006 Newfoundland and Labrador Centre for Health Information, 2009
User	Person, device, program, or computer system that uses a computer system for the purpose of data processing and information exchange.	Canada Health Infoway, *Electronic Health Record Blueprint*, version 2, 2006
User authentication	Process of reliably identifying security subjects by securely associating an identifier and its authenticator. Provision of assurance of the claimed identity of an entity.	ISO 7498-2 *Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture* ISO/IEC 10181-2 *Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework*
User authorization	The permission to perform certain operations or use certain methods or services.	Canada Health Infoway, *Electronic Health Record Blueprint*, version 2, 2006

9. Acknowledgements

The authors gratefully acknowledge the advice and assistance of the following individuals who actively participated in the working group responsible for this document:

Greg Eberhart, BSc. Pharm. CAE
Registrar
Alberta College of Pharmacists

Cameron Egli, BSc (Pharm) ACPR MBA
Director - PharmaNet, eHealth and Technology
College of Pharmacists of British Columbia

Ross Fraser, CISSP, ISSAP
Principal
Sextant Inc.

Sylvain Grenier, CD, B Pharm, PharmD
Commander/Capitaine de Frégate
Chef National de l'exercice en Pharmacie / Pharmacy National Practice Leader
Direction des politiques médicales / Directorate of Medical Policies
Quartier Général du Groupe des Services de Santé des Forces Canadiennes / Canadian Forces Health Services Group Headquarters

Sam Lanctin, BScPharm
Registrar / Secrétaire général
New Brunswick Pharmaceutical Society / Ordre des pharmaciens du Nouveau-Brunswick

Marshall Moleschi, Rph., B.Sc. (Pharm), MHA
Registrar
Ontario College of Pharmacists

Margot Priddle, Ph.C., B.Comm
Registrar
Newfoundland and Labrador Pharmacy Board
formerly Director, Pharmacy Network Program, Newfoundland and Labrador Centre for Health Information

Anne Resnick, R.Ph., B.Sc.Phm., CAE
Deputy Registrar
Ontario College of Pharmacists
formerly Director, Professional Practice Programs, Ontario College of Pharmacists