Canadian Pharmacists Association | Association des Pharmaciens du Canada

cacds
Canadian Association of Chain Drug Stores
Association canadienne des chaînes de pharmacies

JOINT STATEMENT

Recommendations for the Implementation of Electronic Prescriptions in Canada

on behalf of the National e-Pharmacy Task Force

Summary

- Electronic prescribing enhances patient safety.
- Until December 2007, it was the position of Health Canada that amendments to legislation would be required to allow for e-prescribing. After further review, Health Canada concluded that there are currently no regulatory impediments to moving ahead with electronically generated and transmitted prescriptions and that these are permissible to the extent that they achieve the same objectives as written prescriptions.
- In order to ensure patient choice, and the promotion of standard solutions, interoperability and simplified cost-effective implementation, a framework and general policies for electronic prescribing in Canada is required prior to implementation.
- This document outlines the general principles for electronic prescribing from a pharmacy perspective. Pharmacy stakeholders have agreed that these principles should be met by any system used to implement electronic prescribing. It is recognized that pilot projects in Canada for electronic prescribing may not meet the principles outlined in this document.

Background

The National e-Pharmacy Task Force (NePTF) was co-founded by the Canadian Association of Chain Drug Stores and the Canadian Pharmacists Association in 2006. NePTF is composed of two co-chairs and members who represent groups or sectors with a specific interest in the development of e-prescribing, e-dispensing, e-transacting, e-health standards and technologies and their application to the practice of pharmacy.

Significant development in e-health initiatives has occurred at the federal, provincial and territorial levels since the first edition of the e-Prescribing Principles document in 2003.

Most notably from a policy perspective, until December 2007 it was the position of Health Canada that to allow for electronic prescribing (e-prescribing), amendments to Legislation would be required. After

Canadian Pharmacists Association, 1785 Alta Vista Drive, Ottawa, ON K1G 3Y6
www.pharmacists.ca | info@pharmacists.ca | Tel: 1-800-917-9489 613-523-7877 | Fax: 1-800-601-1904 613-523-0445

review, Health Canada concluded that there are currently no regulatory impediments to moving ahead with electronically generated and transmitted prescriptions and that these are permissible to the extent that they achieve the same objectives as written prescriptions. Health Canada's notice on this issue can be found in Appendix A.

In addition, the stable release of the HL7 Version 3 based Pan-Canadian Electronic Drug Messaging Standard (CeRx) has addressed many of the initial areas of concern with e-prescribing by enabling data to be collected and profiled in an electronic health record (EHR) with message specifications to support e-prescribing.

The next priority is to ensure acceptable authentication and security protocols as various jurisdictions begin to implement e-prescribing in the next phases of their e-health agenda, and to ensure that provinces use a standard approach, where feasible, in meeting Health Canada's requirement that provinces and territories wishing to proceed with e-prescribing are obligated to ensure that electronic prescriptions meet existing regulatory requirements and achieve the same objectives as written prescriptions. To realize the principles of this document, stakeholder engagement is critical to ensure that jurisdictions maintain pan-Canadian standards and adopt an authentication method that will achieve regulatory approval, as Health Canada's decision has left the implementation of e-prescribing to the jurisdictions with guidance and funding from Canada Health Infoway.

Infoway created the Electronic Health Record blueprint to serve as a roadmap toward a Canadian system whereby multiple clinicians will write to and access the patient's electronic health profile. NePTF continues to advocate for the use of a centralized provincial drug information system (DIS), which is one of the systems that feeds into the EHR to create a complete patient profile (Appendix B). The first implementation of a drug information system was in British Columbia during the mid 90's, followed by PEI, which was the first jurisdiction to use the CeRx messaging standard for a system-to-system drug information database to enable pharmacy software to directly update the patients profile with dispensing events.

Purpose

This document, *Recommendations for the Implementation of Electronic Prescriptions in Canada*, is a blueprint for the optimal use of e-prescribing. The purpose is to promote a common definition of e-prescribing and encourage jurisdictions to implement a fully electronic e-prescribing system in relation to other e-health initiatives like the provincial drug information systems. In September 2009, NePTF revised the original document published in May 2003 to reflect today's e-health environment. NePTF is well positioned to help guide the six principles described herein by collaborating with pharmacy stakeholders and jurisdictions implementing solutions. The key to the adoption and success of e-prescribing is to ensure pan-Canadian standardization and to advance the use of electronic medical records in physician offices to enable the automation of electronic prescriptions. In order to realize the benefits of e-prescribing it is important to utilize a common method of authenticity.

Defining e-Prescribing

There are several definitions of e-prescribing being developed in Canada and it is important to support a common definition in multiple jurisdictions to ensure consistency among technical solutions. Two leading definitions are from Health Canada, and in the United States, the National Council for Prescription Drug Programs (NCPDP).

NCPDP

NCPDP Definition #1:

Electronic prescribing, as defined by the National Council for Prescription Drug Programs (NCPDP), a standards development organization, has two parts:

Part 1: Two way [electronic] communication between physicians and pharmacies involving new prescriptions, refill authorizations, change requests, cancel prescriptions, and prescription fill messages to track patient compliance. Electronic prescribing is not faxing or printing paper prescriptions.

Part 2: Potential for information sharing with other health care partners including eligibility/formulary information and medication history.[1]

NCPDP Definition #2:

e-Prescribing is the ability of a physician to submit a "clean" prescription directly to a pharmacy from the point of care.[2]

Health Canada

Health Canada defines e-prescribing as a means of streamlining the prescription process by enabling prescriptions to be created, signed and transmitted electronically. There are significant benefits associated with the implementation of e-Rx including the potential to reduce the incidence of medication and dispensing errors caused by illegible prescriptions, a potential decline in adverse drug reactions and the timely transmission of prescription information from practitioner to pharmacist. Health Canada recognizes these benefits and supports the implementation of e-Rx.

NePTF

The National e-Pharmacy Task Force's definition of e-prescribing is: e-Prescribing is the secure electronic transmission from an authorized prescriber of a prescription to a patient's pharmacy of choice integrated with pharmacy software.

Benefits of Electronic Prescriptions

Electronic prescriptions improve patient safety. For example, a leading cause of error is illegible handwriting, or misreading of handwriting on a prescription. Electronic prescriptions eliminate this potential for error.

According to the Institute for Safe Medication Practices (ISMP), "Healthcare practitioners and providers across the nation should rapidly and aggressively take advantage of the electronic prescribing technology that can help prevent medication errors".[3] ISMP believes that electronic prescribing — with proper systems design, implementation, and maintenance can contribute significantly to the prevention of medication errors today.

The Canadian Institute for Health Information's (CIHI) annual report shows that hundreds of lives could be saved every year if Canada had an electronic drug prescription system. It notes approximately 700 deaths in Canada are caused by preventable drug errors each year, many of which could have been avoided if more doctors prescribed drugs online, and that many of the errors are likely caused by doctors' poor handwriting and pharmacists' reluctance to telephone them with questions or the physicians' reluctance to speak directly to the pharmacists to clarify prescription content.

Additional benefits

Improved patient safety outcomes:

- More legible prescriptions informed by physician support tools that reduce the risk of errors.
- Eliminates risk of transcription errors during manual entry at pharmacy.
- Provides information about the appropriateness of the drug being prescribed.
- Reduces adverse drug events and supports delivery of enhanced patient care.
- Availability of complete patient drug profile, patient allergy information and drug-to-drug interactions.
- Supports monitoring of patient adherence through ability to review unfilled e-prescriptions.

Improved process efficiencies:

- Integrated electronic medical record, e-prescribing and patient drug profile enables prescriber to access clinical and formulary information to facilitate timely and informed decision making.
- Alerts and Posted Messages support quicker response to contraindications and medication recalls.
- Reduces call backs between pharmacists and prescribers regarding illegible handwriting, non-formulary medications, potential drug interactions, dosage clarifications, etc.

Principles for e-Prescribing

In 1998 NAPRA developed general recommendations for the safe and effective transfer of patient-specific information and prescription authorization between prescribers and pharmacists using electronic technologies. These recommendations were published in NAPRA's *Report on the Transfer of Authority to Fill Prescriptions by Electronic Transmission.*[4] The report identifies five principles that should be met by systems utilized for electronic prescriptions. NePTF concurs with these principles and jurisdictions, such as Saskatchewan, have adopted similar principles. Health Canada's Therapeutic Products Programme (TPP) has indicated their support for these principles as requirements for the legal transfer of prescription authority and related patient-specific information between prescribers and pharmacists:

1. The process must maintain patient confidentiality.
2. The process must be able to verify the authenticity of the prescription (i.e., the prescriber initiating the prescription).
3. The accuracy of the prescription must be able to be validated, and the process must include a mechanism to prevent forgeries.
4. The process must incorporate a mechanism to prevent diversion, so that the prescription authorization cannot be transmitted to more than one pharmacy.
5. Patient choice must be protected; that is the patient must determine the practitioner to receive the prescription authority by having the prescription stored in a provincial DIS.

Recent implementations and future provincial DIS approaches ensure secure routing of electronic prescriptions in addition to allowing for patient choice. In addition, after completing an environmental scan of all provincial drug information systems that include e-prescribing, it is clear that patient confidentiality and accuracy of the prescription are adequately addressed. As a further safeguard, software vendors must be compliant with the standards implemented through a jurisdictional conformance process that outlines security and implementation protocols.

In addition to the principles, it is important that pharmacists are mandated to record dispensing events into the DIS so that pharmacists realize the benefits of an electronic health record as they will have access to future clinical decision support tools. Accordingly, NePTF has added an additional principle:

6. Pharmacists must have the access and ability to write to the patient profile and other clinical support decision tools.

Proposed Electronic Prescription Security Standards

There are six main components to a secure electronic prescription delivery system:

1. Transaction integrity (digital signature)
2. Data integrity (encryption)
3. Authentication
4. Secure routing (server integrity and intrusion detection).
5. Alternate security structure: the Health Information Access Layer (HIAL)
6. Standards

This document proposes the use of **Public Key Infrastructure (PKI)** as an ideal solution to address transaction and data integrity, two options for authentication, and a number of standards for secure routing.[5]

Ideally a national organization is required to manage the certifications of physicians and pharmacists within the workflow of e-prescribing. However, in the absence of a credible third party able to manage the certification process, combined with the emergence of provincial pharmacy networks and drug information systems, an alternative approach has evolved in some jurisdictions, in part due to the high costs of implementing and maintaining PKI. As a result of e-health initiatives leading to an interoperable electronic health record whereby multiple clinicians use software tools to access a patient's electronic health record, jurisdictions have addressed secure routing and data integrity by implementing a secure infrastructure based on pan-Canadian standards such as the CeRx drug messaging standard and following the Canada Health Infoway (CHI) infostructure for the creation of the Health Information Access Layer (HIAL).

In practical terms, some jurisdictions have chosen another technical approach to PKI for authentication purposes. This approach is either a VPN with user id and password or a client and server certificate, so that only locations that have a client certificate are allowed to send messages and the messages will also be encrypted. In some jurisdictions, like Newfoundland and Labrador, providers will authenticate themselves to the portal using a user id, password, and a number generating token that has been issued to them. When a prescription or a dispense is done from a portal using a web browser instead of directly integrating with the pharmacy application, the provider has to again re-enter their password to complete each prescription as it is written.

NePTF recognizes these alternatives to PKI as acceptable solutions under the condition that a VPN with user id and password is utilized in conjunction with the HIAL as the communication bus layer. Moreover, it is important for the solution to integrate with the pharmacy software to avoid any workflow interruptions.

1. Transaction Integrity

Digital Signature

According to Bill C-6, Part 2: Electronic Documents, "secure electronic signature" means *"an electronic signature that results from the application of a technology or process whereby it can be proved that*:

a) the electronic signature resulting from the use by a person of the technology or process is unique to the person;

b) the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person;

c) the technology or process can be used to identify the person using the technology or process; and

d) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document."

Public Key Infrastructure (PKI) meets all these requirements. PKI allows for non-repudiation, which guarantees that a transaction has taken place and that the parties of the transaction can be identified by their unique digital signatures. Non-repudiation also allows for a comprehensive audit trail. A secure login and password approach that is unique to each prescriber in addition to digital certificates and encryption may also be acceptable for authentication.

2. Data Integrity

Encryption

Encryption ensures the integrity and confidentiality of a transmission by mathematically scrambling the original text so that data cannot be modified or accessed by anyone except an authorized user. Encryption utilizes digital keys (a unique combination of ones and zeros) that are used to encrypt, decrypt and verify digital data.

Public Key Infrastructure

Encryption of data may be accomplished by various technologies. PKI satisfies requirements for digital signature, encryption and the electronic authentication of people. Through the use of a pair of different but related keys, PKI guarantees that a transaction has taken place and that the parties of the transaction can be identified by their unique digital signatures. Each user has a private key and a public key. The private key is kept secure, known only to the user; the other key can be made public and either sent over a net work to each correspondent or, even better, placed in a secure public directory, almost like the electronic equivalent of a telephone book.

PKI technology also uses a combination of algorithms, protocols and derived tools designed for secure communication. To use this kind of system, the sender would encrypt a message with the recipient's public key. Only the recipient's private key could decrypt the message. Public key cryptography therefore

permits the secure transmission of data across open networks such as the Internet without the necessity of previously exchanging a secret key. This allows parties to exchange and authenticate information and conduct business in a secure manner.

Given that this technology ensures the confidentiality, authenticity and validation of prescriptions (Principles of e-prescribing #1, # 2 and # 3, the "Transfer of Authority to Fill Prescriptions by Electronic Transmission"), pharmacy stakeholders strongly recommend that PKI must be implemented for secure transmission of electronic prescriptions. Initial research indicates that a level of security to PKI level 3 provides the safeguards required at a cost that is not prohibitive for implementation.

User Authenticity — Certificate Authorities (CA's) and Registration Authorities (RA's)

In order for public key cryptography to work on a large scale, a trustworthy distribution of public keys is required. This can be accomplished through a **Certificate Authority (CA)**, a trusted entity that manages the distribution of public keys or certificates containing such keys. A "certificate" is an electronic form (similar to an electronic version of a driver's license or a passport) that contains the key holder's public key and some identifying information that confirms that both the key holder and the certificate issuer (the CA) are who they claim to be.

One of the main advantages of having a CA is that it relieves individuals of distributing keys and managing large numbers of relationships in a complex, multiple-security environment. The CA "binds" the specific identity of a key holder to a particular certificate containing the relevant public key by signing the certificate with the CA's key, thereby ensuring authentication and allowing non-repudiation.

Examples of trusted entities that act as Certificate Authorities include Entrust and Verisign.

In addition to a CA, a **Registration Authority (RA)** and Certificate Policies need to be established to implement PKI. An RA screens the authenticity of the people that apply for issuance and revocation of certificates, and provides the interface between the user and the CA. The National Association of Pharmacy Regulatory Authorities (NAPRA) currently maintains a secure and current national database (register) of pharmacists and pharmacies to support its members and their licensing programs. As such, NAPRA has offered to serve as the RA for its members.[6]

3. Authentication

Authentication allows control of user access to a system. Users of an electronic prescription delivery system would require authentication. Examples of mechanisms for authentication include:

1. User name and password authentication

2. Provider, Location and Client Registry.

A provider registry uniquely identifies each caregiver and contains demographic and role information used throughout the EHR solution within a jurisdiction. The role of a registry is to uniquely identify a provider, location and/or patient.[7]

4. Secure Routing

Model of delivery

When routing prescriptions the ability for a patient to maintain their choice of provider is of paramount concern. To preserve patient choice, the delivery of the prescription to the pharmacist is ideal within a provincial pharmacy network directly to a centralized drug-information-system (DIS). The patient arrives at their pharmacy of choice and the prescription is retrieved from the DIS. The method of delivery is either through a secure provider portal or via a system-to-system integration: EMR directly to DIS. The pharmacy software is either integrated with the HIAL which directs the messages to the DIS via a secure pharmacy network or an e-health viewer is provided in the absence of pharmacy software integration (browser).

The recommended standard for electronic prescriptions is a pull model within a system that also allows for push functionality only under specific scenarios:

- Prescriptions are sent by the physician to an approved repository, allowing the pharmacy to retrieve the prescription with the patient's authorization; or
- The prescriber allows the patient to select their preferred pharmacy, and does not influence this decision, nor is the decision influenced by other parties; the prescriber sends prescriptions to any pharmacy that the patient may choose; or
- In the event that the physician is unable to send the prescription electronically to the pharmacy selected by the patient, the physician prints out a hard copy of the prescription for the patient to take to their pharmacy of choice.

5. Alternate Security Standards: the Health Information Access Layer (HIAL)

Provincial e-health initiatives across Canada are utilizing infostructure standards which are the foundation of a pan-Canadian interoperable EHR. The infostructure of an interoperable EHR is a distributed, message-based, peer-to-peer network of EHR systems linking data and services to EHR applications through a common services communication bus (Health Information Access Layer or HIAL). The HIAL platform operates the EHR' s messaging and protocol services, supporting the EHR's domain business components such as Diagnostic Imaging, Laboratory, Pharmacy, Registries — components that capture the information of a patient's medical, drug and lab-testing history. The whole package will result in more accurate diagnosis, safer treatment decisions and speedier access to care for Canadian patients. Use of the HIAL is an acceptable security standard in lieu of implementing PKI.

6. Standards

Any system utilized to implement electronic prescribing should take into consideration the standards being developed within the Standards Collaborative (SC) supported by Canada Health Infoway. The EHR

infostructure, registry and drug standards are maintained within the SC. The SC is responsible for the implementation support, education, conformance, and maintenance for electronic health records (EHR) standards currently being developed by Infoway. There are currently 8 working groups:

- SCWG 2 — Individual Care (Delivery of Care)
- SCWG 3 — Managing the Health System
- SCWG 4 — Medication Management
- SCWG 5 — Labs & Diagnostics
- SCWG 6 — Infostructure & Architecture
- SCWG 7 — Non-clinical Registries
- SCWG 8 — Privacy & IT Security Services
- SCWG 9 — Terminology Representation & Services

Obligation for Data Collection, Disclosure, Use and Protection

Solutions for electronic prescribing must comply with all relevant federal and provincial legislation and regulation.

For example, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) stipulates that private sector organizations must follow a code for the protection of personal information, which is included in the Act as Schedule 1 (Appendix C). The code lists 10 principles of fair information practices which are based on the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information*, and which address the ways in which organizations collect, use and disclose personal information.

It is recommended that any organization that participates in the secure routing of prescriptions must have on file details of how their business ensures privacy, including how it meets the ten principles outlined in the *Model Code for the Protection of Personal Information*.

APPENDIX A

Health Canada Policy Statement on e-Prescribing

December 21, 2007

e-Prescribing (e-Rx) is a means of streamlining the prescription process by enabling prescriptions to be created, signed and transmitted electronically. There are significant benefits associated with the implementation of e-Rx including the potential to reduce the incidence of medication and dispensing errors caused by illegible prescriptions, a potential decline in adverse drug reactions and the timely transmission of prescription information from practitioner to pharmacist. Health Canada recognizes these benefits and supports the implementation of e-Rx.

Until recently, it was the position of Health Canada that, to allow for e-Rx, amendments to Part C of the Food and Drugs Regulations made under the Food and Drugs Act, regulations made under the *Controlled Drugs and Substances Act* and possibly regulations made under *Personal Information Protection and Electronic Documents Act* would be required.

After further review, Health Canada has concluded that there are currently no regulatory impediments to moving ahead with electronically generated and transmitted prescriptions and that these are permissible to the extent that they achieve the same objectives as written prescriptions.

Provinces and territories wishing to proceed with e-Rx are obligated to ensure that electronic prescriptions meet existing regulatory requirements and achieve the same objectives as written prescriptions. For example, there must be evidence of a genuine practitioner/patient relationship, and in the case of controlled substances, pharmacists filling prescriptions must verify prescriptions are signed* by the practitioner before selling or providing drugs containing controlled substances to a patient.

Health Canada has collaborated with Canada Health Infoway on the development of a technical document entitled *Ensuring the Authenticity of Electronic Prescriptions*, in order to provide advice about how to ensure the authenticity of electronic signatures. Although this document (and annexes) was not subject to widespread consultation, it could be of use to provincial and territorial Ministries of Health in moving forward with e-prescribing.

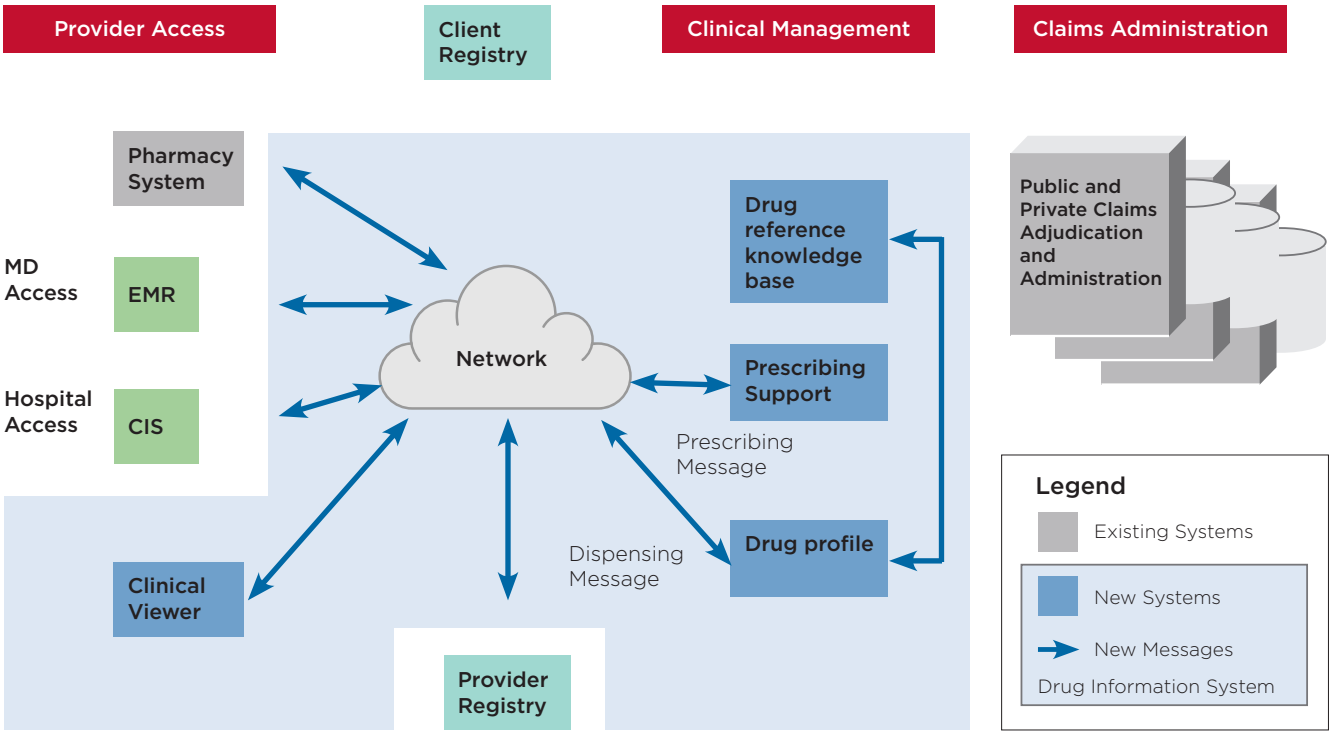
Health Canada has also initiated discussions with provincial and territorial pharmacy and medical regulatory authorities in order to determine how it can be of assistance in facilitating collaboration between provincial and territorial stakeholders regarding e-Rx implementation.

*Sign: 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.

(http://www.hc-sc.gc.ca/hcs-sss/ehealth-esante/e_presc-ord_elec-eng.php)

APPENDIX B

Drug Information Systems (DIS) Infostructure



APPENDIX C

Personal Information Protection and Electronic Documents Act (PIPEDA)

Schedule 1 (Section 5) : Principles set out in the National Standard of Canada, entitled *Model Code for the Protection of Personal Information* (April 13, 2000; CAN/CSA-Q830-96)

4.1 Principle 1 — Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4 Organizations shall implement policies and practices to give effect to the principles, including

a) implementing procedures to protect personal information;

b) establishing procedures to receive and respond to complaints and inquiries;

c) training staff and communicating to staff information about the organization's policies and practices; and

d) developing information to explain the organization's policies and procedures.

4.2 Principle 2 — Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1 The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the consent principle (Clause 4.3).

4.2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6 This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 Principle 3 — Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2 The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3 An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes.

4.3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization,

in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7 Individuals can give consent in many ways. For example:

a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

c) consent may be given orally when information is collected over the telephone; or

d) consent may be given at the time that individuals use a product or service.

4.3.8 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1 Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3 This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

4.5.1 Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4 This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 Principle 6 — Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2 An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4. 7 Principle 7 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3 The methods of protection should include

a) physical measures, for example, locked filing cabinets and restricted access to offices;

b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

c) technological measures, for example, the use of passwords and encryption.

4.7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1 Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2 The information made available shall include

a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

b) the means of gaining access to personal information held by the organization;

c) a description of the type of personal information held by the organization, including a general account of its use;

d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

e) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 — Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2 An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4 An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 Principle 10 — Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1 The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2 Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3 Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4 An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

(http://laws.justice.gc.ca/eng/P-8.6/20090818/index.html)

References

1 "Ready or Not: Gearing Up for the Expansion of ePrescribing," Pharma Marketing News, Vol. 3, #6; REPRINT #36-01.

2 CafeRx Press Release, August 10, 2004; CafeRx Web Site.

3 Call to Action: Eliminate Handwritten Prescriptions Within 3 Years! White Paper from the Institute for Safe Medication Practices 2000.

4 Report on the Transfer of Authority to Fill Prescriptions by Electronic Transmission. *National Association of Pharmacy Regulatory Authorities (NAPRA). March 1998.* http://www.napra.org/Content_Files/Files/electronic.pdf

5 PKI can be defined as a system of digital certificates, Certificate Authorities, and Registration Authorities that verify and authenticate the validity of each party involved in an Internet transaction. Public/private key encryption technology and public key infrastructure (PKI) are examples of technologies and policies that are emerging as de facto standards for the secure exchange of information. Driven by e-commerce and the need for secure communications over the Internet, PKI is rapidly maturing as a security solution in many sectors. Combined with public/private encryption, PKI offers secure confidential communications, authenticity and integrity. Ref: Canadian Institute for Health Information (www.cihi.ca)

6 Members of NAPRA include: Alberta College of Pharmacists, College of Pharmacists of British Columbia, Canadian Forces Pharmacy Services, Manitoba Pharmaceutical Association, New Brunswick Pharmaceutical Society, Newfoundland & Labrador Pharmacy Board, Government of the Northwest Territories, Nova Scotia College of Pharmacists, Ontario College of Pharmacists, Prince Edward Island Pharmacy Board, Ordre des pharmaciens du Québec, Saskatchewan College of Pharmacists, Yukon Government.

7 Canada Health Infoway

Acknowledgements

This document has been adapted from a document developed by a working group of the National Association of Pharmacy Regulatory Authorities (NAPRA): *Proposal for Electronic Prescription Security Standards* (May 10, 2001; http://www.napra.org/Content_Files/Files/erx_security.pdf).

The Canadian Association of Chain Drug Stores and the Canadian Pharmacists Association, on behalf of the National e-Pharmacy Task Force, would like to thank NAPRA and the members of the NAPRA Working Group on Recommendations for Implementation of Electronic Prescription in Canada, for their expertise and time in support of electronic prescribing in Canada.

For further information, contact:

Justin Bates, Director, e-Health
Canadian Association of Chain Drug Stores (CACDS)
jbates@cacds.com; (416) 226-9100

Janet Cooper, Senior Director, Professional and Membership Affairs
Canadian Pharmacists Association (CPhA)
jcooper@pharmacists.ca; (613) 523-7877 x 255