

*A Proposal  
for  
Electronic Prescription  
Security Standards*

*May 10, 2001*

*National Association of Pharmacy Regulatory Authorities*

## Table of Contents

<b>PROPOSED ELECTRONIC PRESCRIPTION SECURITY STANDARDS.....</b>	<b>2</b>
1. TRANSACTION INTEGRITY .....	3
Digital Signature.....	3
2. DATA INTEGRITY.....	3
Encryption .....	3
Public Key Infrastructure .....	3
Confidentiality Certificates .....	4
Responsibilities of Prescribers and Pharmacists .....	5
3. AUTHENTICATION .....	5
4. SECURE ROUTING.....	6
Secure Routing Methods.....	6
Secure Website/Prescription Repository .....	7
Server Integrity .....	7
Intrusion Detection.....	10
Service Level Agreements.....	10
Private Sector Obligations for Data Protection .....	11
<b>CONSULTATION PROCESS FOR REVIEWING THE STANDARDS.....</b>	<b>12</b>
<b>PROPOSED PROCESS FOR IMPLEMENTING THE STANDARDS.....</b>	<b>13</b>
<b>APPENDIX A .....</b>	<b>14</b>
<b>APPENDIX B.....</b>	<b>16</b>

## **PROPOSED ELECTRONIC PRESCRIPTION SECURITY STANDARDS**

These proposed electronic security requirements are informed by *Bill C-6: the Personal Information and Electronic Documents Act and Regulations*, the *Privacy Act*, and *Canada's Evidence Act*.

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

1. Transaction integrity (digital signature)
2. Data integrity (encryption)
3. Authentication, and
4. Secure routing (server integrity and intrusion detection).

This document proposes the use of Public Key Infrastructure to address transaction and data integrity, two options for authentication, and a number of standards for secure routing.

## 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."

To date, the only available technology that satisfactorily meets all of these requirements is **Public Key Infrastructure (PKI)**. PKI offers a non-repudiation feature, 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 offers a comprehensive audit trail. PKI technology is discussed in further detail later in this paper.

## 2. Data Integrity

### Encryption

Encryption provides for the integrity and confidentiality of a transmission by mathematically scrambling the original text so that data cannot be modified without detection. Encryption performs these functions by using digital keys (a unique combination of ones and zeros) that can be employed by an individual user to encrypt, decrypt and verify digital data.

### Public Key Infrastructure

Encryption of data may be accomplished by various technologies but **Public Key Infrastructure** is the only solution that satisfies requirements for digital signature, encryption and the electronic authentication of people. Through the use of a pair of different yet 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 the network 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 thus 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 who do not know each other 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 # 1, 2 and 3 defined by NAPRA), Public Key Infrastructure must be implemented for secure transmission of electronic prescriptions. Policies and guidelines will be developed (as described under Confidentiality Certificates below) to govern the Public Key Infrastructure that is deployed for electronic prescription purposes. It is expected that a recommendation from the APETI working group will be that Government of Canada PKI is used as a standard within the pharmacy supply chain.

The use of Government of Canada PKI has the additional advantage of limiting liability in the event of a legal dispute about a transaction. *Bill C-6, Part 3: Amendments to the Canada Evidence Act* stipulates that *"Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be...The best evidence rule in respect of an electronic document is satisfied ... on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored..."*.

#### Confidentiality Certificates

In order for public key cryptography to work on a large scale, there must be trustworthy distribution of public keys. This can be accomplished through a **certificate authority (CA)**, a trusted agent who certifies the authenticity of users and 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, a passport or a video rental card) containing 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 supporting trusted agent 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 preventing non-repudiation, with the ultimate objective of maintaining confidence in the system.

For the electronic transmission of prescriptions, a Certificate Authority, Registration Authority and Certificate Policies would be established according to the following guidelines:

- an implementation committee (a special subcommittee of NAPRA's National Pharmacy Operations Advisory Committee is proposed) would oversee the initial development and implementation of Certificate Authority policy and procedures,

#### **National Association of Pharmacy Regulatory Authorities (NAPRA)**

- certificate policies would be established with the use of the Public Key Infrastructure Policy Toolkit, published by the Canadian Institute for Health Information (CIHI),
- either the Canadian Imperial Bank of Commerce (CIBC) or Scotiabank could act as the Certificate Authority, (both have already been cross-certified with the root, Health Canada), the chosen CA must also be approved to cross-certify with the Bridge CA (as identified by CIHI)
- in its role as the national association of pharmacy regulatory bodies, it is proposed that NAPRA serve as the Registration Authority. A Registration Authority screens the authenticity of the people that apply for issuance and revocation of certificates and provides the interface between the user and the CA. As a service to its members, NAPRA currently maintains a secure and current national database/register of pharmacists and pharmacies to support provincial licensing programs. Authentication of users would be based on this national register.

#### Responsibilities of Prescribers and Pharmacists

Before being able to submit or receive any prescriptions, prescribers and pharmacists would need to:

- purchase specialized Public Key Infrastructure client software from the CA and install it on their computer system. This software is designed to integrate with common web browsers and is used to digitally sign, encrypt and decrypt web communications (the software will be designed to prompt the user to download and install a 128-bit encryption browser plug-in if it is not already installed,
- contact the certificate authority to register within a central computer functioning as a CA server.

The NAPRA working group envisioned that volume purchasing of software could be facilitated.

### **3. Authentication**

Authentication makes possible the control of user access to a system protected by a particular authentication scheme. Users of the electronic prescription delivery system would have two options for authentication:

1. User name and password authentication (provided by the CA) to access a user's digital certificate, or
2. A biometrics solution could replace the username and password. The PKI software is designed to be compatible with specific biometrics solutions. The implementation committee could research and select the most appropriate biometrics solution(s). Prescribers and pharmacists would be responsible for the cost of purchasing the biometrics hardware and software, to be made available to them by the Certificate Authority. The user would then access their digital certificate with authentication such as using a fingerprint. It has been proposed that the required biometrics hardware and software could also be purchased in bulk to be distributed to pharmacists.

Biometrics may not be warranted when taking into account the security practices built in to existing prescription methodologies.

### **National Association of Pharmacy Regulatory Authorities (NAPRA)**

Users will be made aware that by sharing credentials, they are allowing others to access the prescription system fraudulently and that where a concern relating to the submission of a prescription is raised, the individuals whose digital signatures appear as part of the transactions can be held accountable.

#### 4. Secure Routing

##### Secure Routing Methods

In August 2000, NAPRA commissioned technology consultants at Calian Technology Ltd. to advise on secure methods to electronically deliver prescriptions from prescriber to pharmacist. Calian's report (posted on NAPRA's website at <http://www.napra.org/practice/calian.pdf>) is based on the assumption that delivery will occur in an unmanaged network (e.g. the Internet) and sets out a number of potential internet-based routing solutions.

Two solutions have been identified as complying with the five Principles specified in the "*Transfer of Authority to Fill Prescriptions by Electronic Transmission*":

##### 1. Secure Website Prescription Delivery System

Electronic prescriptions could be delivered via a secure web site, which would function as a centralized electronic prescription routing system. Website providers would need to implement the server integrity and intrusion detection standards outlined later. With this option, the following prescription delivery flow (Appendix A, Diagram 1) would occur:

- √ Prescriber connects to Internet
- √ Prescriber connects to secure web site using web browser and PKI software
- √ Prescriber completes online prescription form (prompt fields, selection lists)
- √ Prescriber submits prescription
- √ Prescription transmitted securely to web site
- √ Pharmacist connects to Internet
- √ Pharmacist connects to secure web site using web browser and PKI software
- √ Pharmacist logs in to web site and retrieves prescriptions

##### 2. Open Interface Prescription Delivery System

Prescribers or pharmacists may prefer to deliver prescriptions via an interface designed by vendors of software applications to integrate with their current health-practice software packages. Such an interface would need to be compatible with the specific PKI security application or technology that is incorporated in the solution.

Prescribers would need to upgrade to a version of their practice software that is designed to work with the "open-interface solution". Additional steps to purchase, install and configure the security software and register the user within a central computer functioning as a CA server would have to be followed.

With this option the following prescription delivery flow (Appendix A: Diagram 2) would occur:

- √ Prescriber connects to Internet
- √ Prescriber connects to secure application server using updated software from existing vendor and PKI software
- √ Prescriber completes online prescription form (prompt fields, selection lists)
- √ Prescriber submits prescription
- √ Prescription transmitted securely to application server
- √ Pharmacist connects to Internet
- √ Pharmacist connects to secure application server using updated software from existing vendor and PKI software
- √ Pharmacist connects to application server and retrieves prescriptions.

The secure web interface would still be available as an option to interface with the prescription routing system as some users may not have access to software that is compatible with this system.

It is proposed that vendors interested in developing an open interface solution would be required to apply to the Implementation Committee for accreditation prior to providing the service and would be bound by the Committee's policies for ongoing system maintenance and certification.

#### Secure Website/Prescription Repository

A secure electronic prescription delivery system also requires an accurate list of pharmacists and pharmacies accredited to receive the prescriptions electronically. A central prescription database or repository for prescriptions, which includes **all** pharmacists and pharmacies licensed in Canada, would be maintained in order to ensure the principle of "patient choice".

As described under "Server Integrity", the server network that will be used to store Pharmacist/Pharmacy information and prescriptions will require a high level of security. The APETI working group is currently defining this level of security.

Potential solutions for prescription repositories would be reviewed by the Implementation Committee to ensure that they meet the standards developed. This committee would oversee the approval/certification of all such repositories in the initial stages of implementation and will develop policies for ongoing certification.

#### Server Integrity

Servers implemented as part of an online prescription delivery solution, and utilized for the storage of sensitive information would need to be protected from compromise. Accordingly, it is imperative that a system designed for the purpose of storing sensitive information be configured with the following considerations:

### 1. Service configuration

The server should be configured to only respond to electronic requests for services that are required for the delivery of information relevant to that server. Making other unrelated electronic entrances available may offer opportunities to exploit the system.

### 2. Access control

Physical and remote access to a particular server should be limited to only those individuals whose responsibilities require their ability to maintain the hardware or the system's electronic configuration as a result of any connectivity related issues.

Individuals responsible for the maintenance and monitoring of the system should be given appropriate access privileges to execute their job functions. If the individual's job must be performed from a remote physical location, a secure method of communication (including both encryption and authentication) should be made available.

The rule of "least privilege" should be implemented to ensure that only the access required to perform one's job function is made available to the individual.

### 3. Firewall Security

Firewalls must be in place to protect all servers deployed as part of the electronic prescription delivery system. The number of firewalls required depends on the security requirements of the system, the technology architecture of the solution, and the concerns of solution stakeholders. Firewalls should be designed to limit the permitted traffic to applications and services that are relevant to the functionality of the online prescription delivery system. Additionally, the firewall should be designed to control the flow of traffic as required for prescription delivery (i.e. traffic requiring inbound access only should not be permitted to travel outbound).

Firewalls that are implemented must be monitored on a regular basis, including regular review and analysis of generated log files. Designated administrators should be sure to keep the firewall configuration and software patching level current as per the vendor's advisories on security matters relating to their product.

No means to bypass firewall security should be made available. This includes any inbound or outbound modem connections to any servers connected to the protected network.

### 4. Hosting

Any server hosting should have clearly defined levels of service that include, but are not limited to the following key areas of concern:

- **Physical Security:** Physical access to the servers should be limited to employees, contractors and consultants who have passed a security screening. For best security, access should be controlled

using doors secured by magnetic key card technology. In all cases, policies regarding discipline for the sharing of key cards and/or cipher lock combinations should be documented and enforced.

- **Availability:** The hosting provider should ensure that the system(s) remain Internet accessible 98.5% of the time, seven days a week. This reflects typical uptime guarantees offered by established hosting providers.
- **Monitoring:** The hosting provider should monitor the system(s) around the clock and respond within a specified period of time to any warnings, errors and failures reported by any relevant monitors. Additionally, all levels of alerts should be resolved within a specified period of time. Guidelines for this can only be established in relation to any specialized hardware support agreements available and purchased.
- **Reporting:** The hosting provider should maintain a number of up-to-date graphs at all times. These should include (but not be limited to): bandwidth consumption, throughput, response times and system availability. Hardcopy graphs, summaries of any monitoring alerts, open service calls and closed service calls should be furnished by the hosting provider each month.
- **Environment:** The hosting provider should guarantee a monitored, climate-controlled environment that meets the requirements of the hardware used for the service.
- **Power:** The hosting provider should guarantee reliable and clean power for the hosted equipment. Monitored battery backups and backup generators should be available to substantially reduce the risk of power related failures.
- **Data backup:** The hosting provider should be contracted to perform nightly backups of the data on all systems. Backup media should be rotated regularly and copies of the media should be stored securely off-site. In the event of a failure of a system disk or other data loss on the system, the hosting provider should be able to restore the lost data from the most recent backup in a timely manner.

#### 5. Technical Administration

Once a system is in place, routine maintenance will be crucial in keeping the system operational, and user access and vendor patching current. The following issues need to be considered when planning a maintenance infrastructure:

- **System performance:** Hardware and operating systems should be checked regularly for any obvious problems relating to reliable performance.
- **Log file analysis:** Many hardware components, operating systems and software applications generate activity reports and error logs in the form of data files on a disk drive. Routine

examination of these files can help determine any ongoing or potential problems that need to be addressed.

- Patch application: Hardware and software vendors routinely issue updates to their released software. In many cases the patches relate to features or functionality. However, in some cases the updates address specific security issues that can pose significant threats. Regular review of available vendor patches is imperative.

## 6. Technology Selection

Where a decision relating to the selection of a particular technology is concerned, standards-based solutions should be selected whenever possible. Standards based technology is typically defined by a regulatory body or association of key industry players. An example of an organization that publishes standards for technology is the Internet Engineering Task Force (IETF). Other considerations are industry recognized certifications such as those obtained from the International Computer Security Agency (ICSA).

### Intrusion Detection

At the minimum, host-based intrusion detection software should be installed on the central servers. Host based intrusion detection ensures that a particular system is protected from known forms of attack. The required detection software is installed on the protected host and monitors all calls for electronic interaction and logs any suspicious activities to a data file. Additional alerts can be sent to administrators by email or pager.

If the number of servers required for the system exceeds four and security of patient data is paramount, network based intrusion detection software should also be implemented. Network based Intrusion Detection ensures interconnected systems are protected from known forms of network-based attacks. The required detection software is installed on a system dedicated to monitoring the network, and monitors all network activity. All suspicious activity can be logged to data files. Additional alerts can be sent to administrators by email or pager.

Ideally, the network based intrusion detection system selected will integrate at the network perimeter firewall.

### Service Level Agreements

When engaging the services of a third-party vendor, all approved parties must implement Service Level Agreements (SLAs) with vendors that clearly defines the roles of both the vendor and the organization in making an electronic prescription available. Typically, SLAs document the agreed-to commitments of the various organizations in making the system available on an ongoing basis. Additionally, the SLAs should identify accountabilities and penalties for failure to deliver services to a measurable degree of satisfaction.

### Private Sector Obligations for Data Protection

*Bill C-6: the Personal Information and Electronic Documents Act* 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 B). 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.

The *Model Cross-Jurisdictional Privacy Impact Assessment (PIA) Guide* provides a methodological framework to ensure privacy is ensured throughout a project development cycle. The PIA process has the following components:

- Data Analysis Documentation: a business process diagram and data flow tables to analyze from a data protection viewpoint how and by whom personal information will be collected, used and disclosed.
- Privacy Analysis Documentation: an analysis of the data flow and potential privacy issues against the 10 privacy principles in the CSA Model Code and relevant privacy laws and policies to determine and document the privacy implications and risks of the proposal
- Privacy Risk Management Plan: a documented evaluation of the privacy implications and risks with actions, recommendations and/or options to mitigate the risks including a high level policy-based discussion of the electronic service delivery proposal and privacy.

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 10 principles outlined in the *Model Code for the Protection of Personal Information*. This documentation must also include:

- a design and implementation document that details the security components that are implemented and the way in which they will be configured, and
- a security policy document which should be made available to all individuals tasked with implementing and maintaining the electronic prescription delivery system. This document should present the sharing of trusted access to the system as unacceptable.

## **CONSULTATION PROCESS FOR REVIEWING THE STANDARDS**

These draft standards are being distributed on both a national and provincial basis. NAPRA is overseeing distribution to:

- national pharmacy, medical, dental, and veterinary associations,
- national health information groups,
- the pharmaceutical industry,
- the Therapeutics Product Program, and
- other interested national stakeholders representing areas within the pharmacy supply chain.

NAPRA's member provincial and territorial pharmacy regulatory authorities will be responsible for the distribution of these draft standards at the provincial/territorial level.

Comments will be considered by the NAPRA working group and the standards revised in accordance with feedback received. If warranted, a further consultation process may be undertaken.

## PROPOSED PROCESS FOR IMPLEMENTING THE STANDARDS

The following steps are proposed to implement standards for secure transmission of electronic prescriptions from prescriber to pharmacist. Actual dates will depend on the release date of the APETI paper and on the feedback received from this initial consultation.

It has been proposed that a special subcommittee of the National Advisory Committee on Pharmacy Operations will be formed to oversee the implementation of these standards.

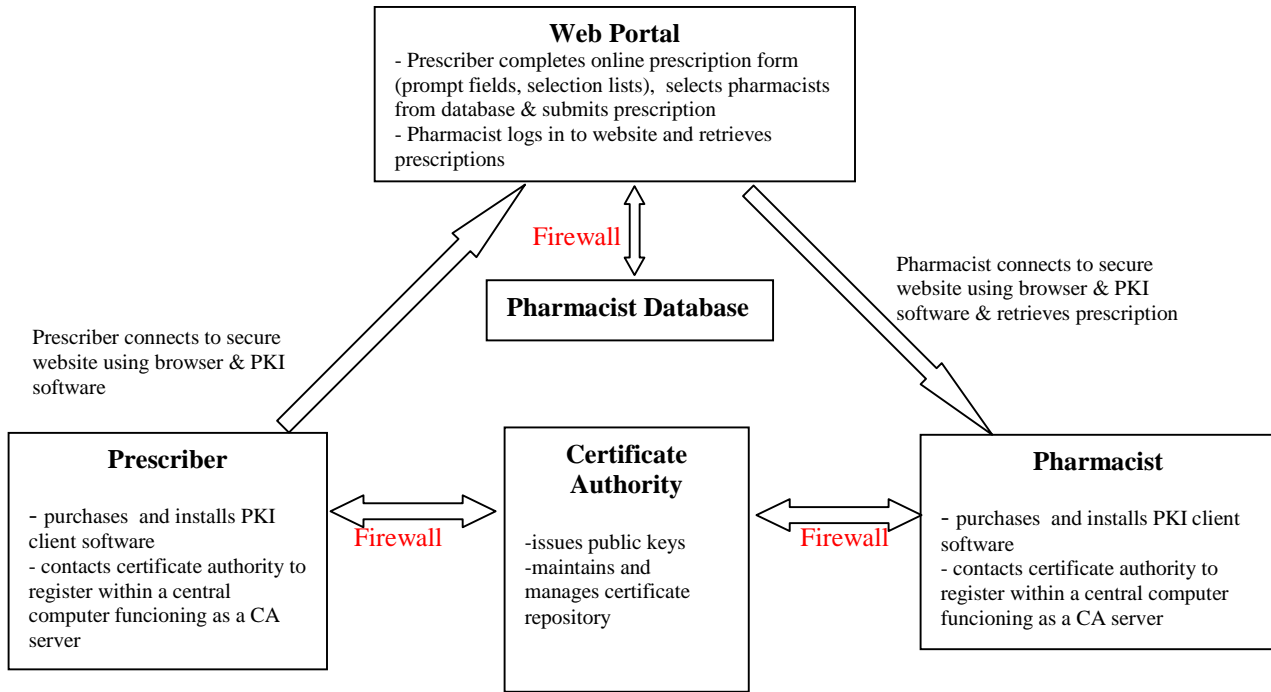
This subcommittee will be responsible for:

- developing policies and related procedures required for implementation of these standards during the initial set-up of the secure electronic prescription transmission system in Canada, including:
  - digital signature and confidentiality certificate policies for Public Key Infrastructure relating to electronic transmission of prescriptions,
  - authentication protocol, and
  - certification of secure prescription repository(s)/databases for storage of electronic prescriptions during transmission.
- selecting technical experts for consulting purposes (preferably technical expertise from both within and outside the pharmacy industry)
- developing standards and policies for ongoing system maintenance and certification upon completion of the initial set-up.

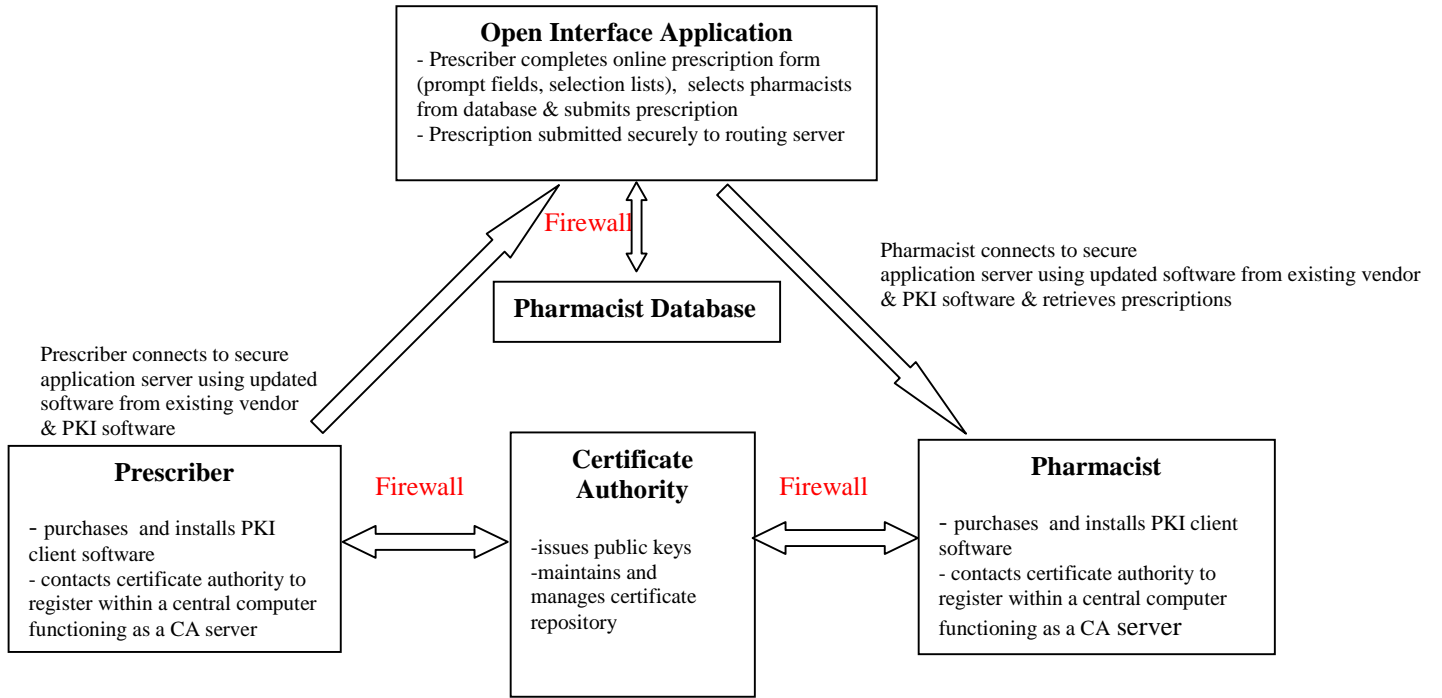
There will be a format established for interested vendors to present technical solutions, and to provide input and technical expertise into the process.

## Appendix A

**Diagram 1**  
**Secure Web Prescription Delivery System**



**Diagram 2**  
**Open Interface Delivery System**



## APPENDIX B

### SCHEDULE 1 (Section 5)

#### PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION, 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.