

## 9 Privacy

9.1	Positive Identification of Patients .....	3
	<i>Requirements for Identification</i> .....	3
	<i>Primary Identification</i> .....	3
	<i>Secondary Identification</i> .....	4
	<i>Identification when managing patient protective words</i> .....	4
	<i>Protecting patient information from fraudulent use or identity theft</i> .....	4
9.2	Confidentiality Agreements .....	5
	<i>Pharmacy Confidentiality Agreements</i> .....	5
	<i>Medical Practice Confidentiality Agreements</i> .....	6
	<i>Emergency Department Confidentiality Agreements</i> .....	7
	<i>Hospital Confidentiality Agreements</i> .....	7
	<i>Medical Device Distributor Confidentiality Agreements</i> .....	8
	<i>Ministry of Health and Health Insurance BC Confidentiality Agreements</i> .....	8
9.3	Access to Patient Information .....	9
	<i>Access by Pharmacists</i> .....	9
	<i>Access by the College of Pharmacists</i> .....	10
	<i>Access by Emergency Departments</i> .....	10
	<i>Access by Medical Practices</i> .....	10
	<i>Access by Hospitals and Designated Mental Health Facilities</i> .....	11
	<i>Access by Device Providers</i> .....	11
	<i>Access by Patients</i> .....	11
	<i>Access for Research</i> .....	12
	<i>PharmaNet Access Restrictions</i> .....	12
	<i>Locale and Site Access Restrictions</i> .....	12
	<i>Device Restrictions</i> .....	12
9.4	Wireless Access .....	13
	<i>Submitting a signed attestation</i> .....	13
	<i>Attestation term limits</i> .....	14
	<i>Failure to comply</i> .....	14

9.5	Patient Records.....	15
	<i>Patient Data Stored on PharmaNet.....</i>	<i>15</i>
	<i>Patient Record Access.....</i>	<i>15</i>
	<i>Patient Requests to View their Own Data.....</i>	<i>15</i>
	<i>Procedures for pharmacists and medical practices.....</i>	<i>16</i>
9.6	Protective Words.....	18
	<i>Protective Word Requirements.....</i>	<i>18</i>
	<i>Access to Protected PharmaNet Records.....</i>	<i>18</i>
	<i>Emergency Access if Protective Word Not Known.....</i>	<i>19</i>
	<i>Adding, removing or changing a protective word.....</i>	<i>19</i>
	<i>Who may request a protective word at a community pharmacy.....</i>	<i>19</i>
	<i>Acceptable Proofs of Identity when Managing Patient Protective Words.....</i>	<i>19</i>
	<i>Protective Word Removal.....</i>	<i>21</i>
	<i>Creating a Protective Word.....</i>	<i>21</i>
	<i>Storing and Sharing Patient Protective Words.....</i>	<i>22</i>
	<i>Procedures for Pharmacies.....</i>	<i>23</i>
	<i>Adding a Protective Word to a Patient’s Own PharmaNet Record.....</i>	<i>23</i>
	<i>Removing a Protective Word From a Patient’s Own PharmaNet Record.....</i>	<i>23</i>
	<i>Changing a Protective Word on a Patient’s Own PharmaNet Record.....</i>	<i>23</i>
9.7	PharmaNet Security.....	25
	<i>Overview.....</i>	<i>25</i>
	<i>Physical Security.....</i>	<i>25</i>
	<i>Operating System Security.....</i>	<i>25</i>
	<i>Network Security.....</i>	<i>26</i>
	<i>Transaction Security.....</i>	<i>26</i>
	<i>PharmaNet Screen Security.....</i>	<i>26</i>

## 9.1 Positive Identification of Patients

[June 1, 2015: Updated to reflect the Information Management Regulation]

### General Policy Description

The *Pharmacy Operations and Drug Scheduling Act* (PODSA) bylaw 22 requires pharmacists to take reasonable steps to positively identify a patient, patient's representative, pharmacist or a practitioner before providing any pharmacy service.

### Policy Details

#### Requirements for Identification

- The *Pharmacy Operations and Drug Scheduling Act* (PODSA) bylaw 22 requires pharmacists to take reasonable steps to positively identify a patient, patient's representative, pharmacist or a practitioner before providing any pharmacy service, including but not limited to:
  - obtaining prescription services for the first time in each pharmacy
  - establishing a patient record
  - updating clinical information on a patient record
  - establishing, deleting or changing a patient **protective word**
  - providing a printout of an in-pharmacy patient record or requesting a PharmaNet patient record from the College of Pharmacists of British Columbia (CPBC)
  - establishing, deleting, or changing a patient **protective word**
  - viewing a patient record
  - answering questions regarding the existence and content of a patient record
  - correcting information, and
  - disclosing relevant patient record information to another pharmacist for the purpose of dispensing a drug or device, and/or for the purpose of monitoring drug use.
- CPBC Professional Practice Policy 54 - Identifying Patients for PharmaNet Purposes establishes:
  - Pharmacists must ensure that only one PharmaNet patient record is created and maintained for each person and that only one Personal Health Number (PHN) is assigned to each person. By viewing and confirming appropriate identification documents, duplicate PHNs and patient records can be avoided
  - where a patient is personally known to the pharmacist for a period of two years or longer, the pharmacist may positively identify the patient, and
  - if the patient is not known to the pharmacist, positive identification is best achieved by viewing one piece of primary identification or two pieces of secondary identification.

#### Primary Identification

- CPBC Professional Practice Policy 54—Identifying Patients for PharmaNet Purposes establishes the following as primary identification:
  - Driver's License
  - Passport

- Provincial Identity card issued by the Province of BC
- Police Identity Card issued by RCMP or Municipality
- Certificate of Indian Status Card

### **Secondary Identification**

- CPBC Professional Practice Policy 54—Identifying Patients for PharmaNet Purposes establishes the following as secondary information:
  - CareCard issued by the Province of B.C.
  - Birth Certificate
  - Canadian Citizenship Card
  - Landed Immigrant Status papers
  - Naturalization Certificate
  - Marriage certificate
  - Change of Name Certificate
  - Identification or Discharge Certificate from External Affairs Canada or Canadian Armed Forces
  - Consular Identity Card

### **Identification when managing patient protective words**

- **Separate identification requirements apply when managing patient protective words (i.e., when applying, removing or changing a protective word on the patient’s own PharmaNet record).**  
 >> **See [Section 9.6](#) for details.**

### **Protecting patient information from fraudulent use or identity theft**

- Pharmacists are asked to refuse phone requests for pharmacy or patient information if they cannot positively identify the caller. Such requests are often consistent with an attempt to obtain drugs illegally or to commit identity theft.
- Pharmacies are also asked to report to HIBC any suspicious requests they receive. In particular, if a caller claims to be from PharmaCare, PharmaNet or HIBC, please confirm their identity by calling HIBC directly before you respond to their request.
- **Please note that HIBC does not contact pharmacies to ask for pharmacy identifiers.**
- HIBC continues to carefully screen callers using the standard verification procedures. To help prevent misuse of pharmacy or pharmacist identifiers, when calling the [PharmaNet Help Desk](#) at HIBC, please be prepared to provide any information necessary to substantiate your identity.

### **Tools and Resources**

- College of Pharmacists of BC: [Identifying patients for PharmaNet purposes.](#)
- College of Pharmacists of BC: [PODSA bylaws](#)

## 9.2 Confidentiality Agreements

### General Policy Description

All PharmaNet users with access to patient information are required to sign confidentiality agreements.

Confidentiality agreements are intended to:

- document the user's agreement to adhere to all legislation, policies, procedures and standards related to the confidentiality, privacy and security of patient and clinical information in PharmaNet
- document requirements and responsibilities for the protection of patient information
- identify limits on access to patient information
- identify individuals authorized to access patient information
- ensure access to patient information is properly managed
- document that all required measures to protect privacy have been undertaken
- protect the user from any legal issues that may arise.

### Policy Details

#### Pharmacy Confidentiality Agreements

- Pharmacies are required to comply with the policies and administrative requirements with regard to pharmacy confidentiality agreements established by the College of Pharmacists of British Columbia, which include the following:
  - Every person who has access to the dispensary must complete the appropriate confidentiality agreement.
  - In the process of completing the confidentiality agreement, the pharmacy manager should explain to each person the reason for its completion and the confidential nature of dealings within the dispensary.
  - The confidentiality agreement appropriate for each person who has access to the dispensary is to be used:
    - **Registrant Confidentiality Undertaking.** This form is signed by each registrant registered with the College of Pharmacists of BC and is maintained on file by the College.
    - **Designated Non-Pharmacist Owner, Non-Pharmacist Store Manager and/or Director Confidentiality Undertaking.** This form is to be completed by a non-pharmacist storeowner, a non-pharmacist store manager or company director who has access to the dispensary.
    - **Pharmacy Designated Support Person Confidentiality Undertaking.** This form is used for a support person and any other store personnel who have access to the dispensary. This form should also be completed by anyone who accesses the dispensary after hours in the absence of the pharmacy manager, including janitors or overnight merchandising staff.
    - **PharmaNet Third-Party Confidentiality Undertaking.** This form is to be completed by the pharmacy software vendor, who may also have special authorized remote access capabilities.

>> Copies of pharmacy confidentiality agreements are available on the [College of Pharmacists of BC PharmaNet Forms website](#).

- Completed forms should be retained by the pharmacy while the staff member is employed and for at least three years after their employment ceases for CPBC purposes. PharmaCare requires these documents to be retained for four years.
- The signing of one agreement covers a pharmacist for all stores he/she may work in, as long as the undertaking is on file at the College.
- It is the pharmacy manager's responsibility to ensure that everyone understands the forms being signed and that all staff comply with confidentiality procedures.
- Each pharmacy must have a system in place to ensure that undertakings are signed on a regular basis, filed within the pharmacy, and made available to College representatives.
- A copy should be given to the employee and the original filed in the pharmacy.
- Designated support persons who work at more than one pharmacy must sign a confidentiality undertaking at each pharmacy, even if all the pharmacies are part of the same chain.

>> For further information see the College of Pharmacists of BC: [PharmaNet Confidentiality Q&A](#) or contact the CPBC.

### Medical Practice Confidentiality Agreements

[June 1, 2015: Updated to reflect the Information Management Regulation]

- Medical Practice Access to PharmaNet (MPAP) allows authorized medical practitioners to receive up-to-date records of medications dispensed to a patient, in a timely and secure manner, at each registered practice site.
- Physicians may register to access PharmaNet from one or more sites at which they practice. They may access PharmaNet only from within the sites for which they have registered.
- Physicians who wish to access PharmaNet from health authority facilities must do so using Hospital Access to PharmaNet or Emergency Department Access to PharmaNet.
- To be eligible to register for MPAP access, physicians
  - must deliver direct patient care at a medical practice site in British Columbia, and
  - must be in good standing with their college.
- Each eligible physician must comply with the terms of the Community Health Practitioner PharmaNet Access Agreement. The Agreement and its companion documents are to be completed, signed and submitted in the manner established at the [Medical Practice Access to PharmaNet](#) website before access will be granted.
- If a supervised person (or persons) will be accessing PharmaNet on behalf of the practitioner, the supervised person(s) must sign an Undertaking of Confidentiality and Security. These documents must be retained on site at the practice for auditing purposes.

## ***Emergency Department Confidentiality Agreements***

- Emergency Department Access to PharmaNet (EDAP) permits authorized individuals in hospital emergency departments, and diagnostic and treatment centres, to access patient medication profiles to assist in determination of patient therapy, in a timely and secure manner.
- EDAP requires compliance with the confidentiality undertaking requirements established in the [PharmaNet Professional and Software Compliance Standards Volume 2–Business Rules: Emergency Departments](#), which include:
  - confidentiality undertakings for physicians authorized to access PharmaNet information in the emergency department
  - confidentiality undertakings or pledges of confidentiality for nurses and clerical employees authorized to access PharmaNet information in the emergency department
  - confidentiality undertakings with technical support staff who may have access to PharmaNet through the course of their duties
  - an Emergency Department Access to PharmaNet Acknowledgement of Completion of Confidentiality Procedures.

>> See the [Emergency Department Access to PharmaNet](#) website for further information.

## ***Hospital Confidentiality Agreements***

- Hospital Access to PharmaNet (HAP) allows authorized physicians and pharmacists to request and receive up-to-date records of medications dispensed to a patient, in a timely and secure manner, at each registered hospital or designated mental health facility (DMHF).
- HAP requires compliance with the confidentiality undertaking requirements established in the [PharmaNet Professional and Software Compliance Standards Volume 2 – Business Rules - Hospital](#) and the [Hospital Access to PharmaNet Policies and Procedures](#), which include:
  - the hospital must complete and submit to the Ministry of Health an Undertaking to Complete Confidentiality Procedures for Hospital Access to PharmaNet.
  - each physician accessing PharmaNet in the **facility** must be a member in good standing with the College of Physicians and Surgeons of British Columbia and sign an Undertaking of Confidentiality and Acknowledgment of Disclaimer by Physician for Hospital Access to PharmaNet. This document is retained by the **facility**.
  - each **supervised** person acting on the physician's behalf in the **facility** must sign an Undertaking of Confidentiality and Acknowledgment of Disclaimer by Authorized Person for Hospital Access to PharmaNet. This document is retained by the **facility**.
- No additional confidentiality undertaking is required for pharmacists since they have already signed a confidentiality undertaking which is retained by the College of Pharmacists of British Columbia.
- Further information and copies of undertakings are available from the [Hospital Access to PharmaNet](#) website.

### ***Medical Device Distributor Confidentiality Agreements***

- Medical Device Distributor Claims Access to PharmaNet permits the submission of claims for eligible devices and supplies on PharmaNet.
- Medical Device Distributor Claims Access requires compliance with the confidentiality undertaking requirements established in the [Medical Device Distributor Claims Access to PharmaNet Policies and Procedures](#), which include:
  - completion and submission to the Ministry of Health of an Acknowledgement of Completion of Confidentiality Procedures for Medical Device Distributor Claims Access to PharmaNet (HLTH 4551 form).
  - the manager must complete a Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Manager (HLTH 4549 form).
  - before accessing PharmaNet, each authorized staff member must complete and sign a Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Authorized Person (HLTH 4550 form).
  - before the Medical Device Distributor manager allows any software vendor technician or staff to access PharmaNet, he/she must obtain a completed and signed *Medical Device Distributor - Software Vendor PharmaNet Third Party Confidentiality Undertaking* form.

>> Copies of forms along with completion and submission instructions are available at the [Medical Device Distributors \(MDD\) Online Claims Access to PharmaNet](#) website.

- A copy of all completed documents is to be maintained on file at the MDD site.

### ***Ministry of Health and Health Insurance BC Confidentiality Agreements***

- All Ministry of Health and Health Insurance BC staff members or service providers who may handle or have access to confidential PharmaNet information or documents are subject to confidentiality provisions as a term of their employment or contract.



## 9.3 Access to Patient Information

[June 1, 2015: Updated to reflect the Information Management Regulation]

### General Policy Description

Access to patient information on PharmaNet is subject to [the \*Pharmaceutical Services Act, Information Management Regulation\*](#) and the *Pharmacy Operations and Drug Scheduling Act* (PODSA). Pursuant to PODSA, the Ministry of Health is responsible for the management of PharmaNet.

PharmaNet was developed to address the diverse needs of individuals and organizations using it. Some users need “update” access to specific parts; others may require “read-only” access to specific information.

PharmaNet information is stored and managed by two separate computer systems, the Drug Information System (DIS) and the PharmaCare Centralized Information System (PCIS):

- The DIS component contains patient medication histories and drug information and is under the custodianship of the Ministry of Health. Drug information updates are supplied by First Databank.
- The PharmaNet Help Desk (operated by Health Insurance BC) does not have access to DIS. The PharmaNet Stewardship Committee handles enquiries regarding access to the DIS.

The PCIS component contains patient claims and expenditure information and is under the custodianship of the Ministry of Health.

The PharmaNet system’s Coordination of Benefits (CoB) Router accepts a user's submitted dispensing claim transaction and automatically routes it to and from the appropriate application systems on PharmaNet. PharmaCare can access CoB information.

Dispensing claim information is directed to PCIS for adjudication and to the DIS system for Drug Use Evaluation (DUE) and medication details. Results from each of these systems are then sent back to the CoB Router and are transmitted to the user's local system.

### Policy Details

#### Access by Pharmacists

- The [Pharmaceutical Services Act and its Information Management Regulation](#) permit pharmacists to access personal health information on PharmaNet.
- The PODSA Bylaw 21 limits registrants of the College of Pharmacists of BC (CPBC) to accessing a patient's PharmaNet record only:
  - to dispense a drug,
  - to provide patient consultation,
  - to evaluate a patient's drug usage, and/or
  - for the purposes of claims adjudication and payment by an insurer.
- Once a year every pharmacy in British Columbia undergoes a PharmaNet access audit conducted by the CPBC to ensure pharmacists are accessing PharmaNet records only for appropriate reasons.

### Access by the College of Pharmacists

- The *Pharmaceutical Services Act* permits the College of Pharmacists of BC (CPBC) to access personal health information on PharmaNet for specified purposes, including the monitoring by the CPBC of the practice of pharmacy.

### Access by Emergency Departments

- Emergency Department Access to PharmaNet (EDAP) permits authorized individuals in hospital emergency departments, and diagnostic and treatment centres, to access patient medication profiles to assist in determination of patient therapy.
- Emergency Department (ED) practitioners and supervised persons who access PharmaNet on their behalf may add the following to the patient's medication history:
  - notes on adverse drug reactions, allergies and clinical conditions
  - entries for drugs dispensed in the ED (using the TMU transaction)
- Access to PharmaNet patient information in emergency departments and diagnostic treatment centres is subject to the *Pharmaceutical Services Act*, [Information Management Regulation](#) and *Pharmacy Operations and Drug Scheduling Act*.
- The access to patient information must be in compliance with [PharmaNet Professional and Software Compliance Standards Volume 2—Business Rules: Emergency Departments](#).
- The Compliance Standards identify the patient information that may be accessed, and requirements for monitoring access.

>> See the [Emergency Department Access to PharmaNet](#) website for further information.

### Access by Medical Practices

- Medical Practice Access to PharmaNet (MPAP) allows authorized medical practitioners to receive up-to-date records of medications dispensed to a patient, in a timely and secure manner, at each registered practice site.
- Physicians may register to access PharmaNet from one or more sites at which they practice. They may access PharmaNet only from within the sites for which they have registered.
- Physicians who wish to access PharmaNet from health authority facilities must do so using Hospital Access to PharmaNet or Emergency Department Access to PharmaNet.
- Access to PharmaNet patient information by medical practices is subject to the *Pharmaceutical Services Act* and its [Information Management Regulation](#).
- To be eligible to register for MPAP access, physicians
  - must deliver direct patient care at a medical practice site in British Columbia, and
  - must be in good standing with their college.
- Each eligible physician must comply with the terms of the [Community Health Practitioner PharmaNet Access Agreement](#). The Agreement and its companion documents are to be completed, signed and submitted in the manner established at the [Medical Practice Access to PharmaNet](#) website before access will be granted.

- If a supervised person (or persons) will be accessing PharmaNet on behalf of the **practitioner**, the supervised person(s) must sign an Undertaking of Confidentiality and Security. These documents must be retained **on site at the practice** for auditing purposes.
- The access to patient information must **also** be in compliance with the [Professional and Software Compliance Standards Volume 2 Business Rules—Medical Practice](#). The Compliance Standards identify the patient information that may be accessed and requirements for monitoring access.

>> See the [Medical Practice Access to PharmaNet](#) website for further information.

### **Access by Hospitals and Designated Mental Health Facilities**

- Hospital Access to PharmaNet (HAP) allows authorized individuals to access patient medication histories from a hospital or designated mental health facility.
- **Practitioner access** to PharmaNet patient information in hospitals and designated mental health facilities is subject to the *Pharmaceutical Services Act and its Information Management Regulation*.
- The access to patient information must be in compliance with [PharmaNet Professional and Software Compliance Standards Volume 2—Business Rules: Hospital](#).
- The Compliance Standards identify the patient information that may be accessed and requirements for monitoring access.

>> See the [Hospital Access to PharmaNet](#) website for further information.

### **Access by Device Providers**

- **Device providers enrolled in the PharmaCare program** may be granted access to PharmaNet to submit online claims to PharmaCare. For example, prosthetic and orthotic suppliers, ostomy suppliers, mastectomy suppliers, medical device distributors and medical supply stores.
- **Device providers** are not granted access to full patient medical histories.

### **Access by Patients**

- A patient may request a printed copy of their confidential and personal data from either a local pharmacy system, or from PharmaNet, or both. A patient may request a copy of either through any community pharmacy.
- **Note: The local system record from a pharmacy contains only those medications that were dispensed by the pharmacy at which the request is made.**
- **The PharmaNet patient record does not contain any medication expense or PharmaCare coverage information.**
- **Patients may request either:**
  - **a current PharmaNet patient record**—includes the patient’s demographic information, clinical information, adverse reaction information, medication history of the last 15 prescriptions within the last 14 months or for the last 14 months and a log of all persons who have accessed the patient’s information when no medication was dispensed

- **an archived patient record**—includes a record of medications dispensed before the most recent 14 months. Records can be requested from September 1, 1995, onward (when PharmaNet was implemented).
- While a community pharmacy can print a patient’s locally stored record, it cannot print the PharmaNet patient record. Instead, the pharmacy must submit the request to the College of Pharmacists of British Columbia which, in turn, mails the information directly to the patient. Pharmacists can use their local system software to request the PharmaNet record.
- Access to a patient record without the filling of a prescription results in a documented access. The PharmaNet patient record lists each access to a patient record that is not associated with a prescription fill.

Refer also to [Patient Requests to View their Own Data](#).

### Access for Research

- Access to PharmaNet patient information for the purpose of research is subject to the *Pharmaceutical Services Act*.
- Research access is overseen by the **Data** Stewardship Committee (DSC). The DSC also reviews requests to use PharmaNet data to contact individuals to request participation in health research **prior to their assessment by the Office of the Information and Privacy Commissioner**.

>> See the [Data Stewardship Committee](#) website for further information.

### PharmaNet Access Restrictions

- **These restrictions ensure patient privacy is protected according to B.C. legislation.**

#### **Locale and Site Access Restrictions**

- To comply with the terms of the *Freedom of Information and Protection of Privacy Act* (RSBC 1996) and *Personal Information Protection Act* (SBC 2003 C. 63), access to PharmaNet can be granted only to sites located in British Columbia.
- Any online PharmaNet claim must be processed by the B.C. site (that is, it cannot be processed remotely from another location) and any personal information derived from that **claim or from PharmaNet in general** must remain in B.C.
- **No one may access PharmaNet outside the premises of a registered site. All access must be made within the premises, even if the site is authorized to use a secure wireless Local Area Network whose coverage extends beyond the boundaries of the premises.**

#### **Device Restrictions**

- **No one may access PharmaNet by means of a wireless mobile device such as a laptop, smartphone or tablet unless the device is 100% owned by a registered practice or facility and is fully compliant with the government’s information management and security requirements for equipment and infrastructures. The devices must be tested and approved by the Ministry of Health before use.**

## 9.4 Wireless Access

### General Policy Description

The Ministry of Health allows wireless access to PharmaNet from **tested**, secure wireless Local Area Networks, **subject to the [PharmaNet Access Restrictions](#) cited above.**

### Policy Details

- To use wireless access to connect to PharmaNet, users/facilities must:
  1. Comply with Office of the Chief Information Officer (OCIO) wireless standards.
    - Secure wireless Local Area Networks and equipment must comply with the wireless standards specified by the OCIO of BC as set forth in the [Information Management/Information Technology Standards Manual](#).
  2. Provide appropriate staff training.
    - All new and current employees must be provided with information about the facility's wireless policy and procedures as they relate to access to PharmaNet.
  3. Ensure proper incident reporting.
    - Users/facilities must ensure that employees report all information security incidents to whoever signed the Attestation of Compliance. Security incidents are defined in the [Government of British Columbia's Information Security Policy](#).
    - Any incidents must be handled in accordance with the OCIO wireless standards.
  4. Complete an Attestation of Compliance.
    - Attestation forms are available through the [System Access Services](#) website.

### Procedures

#### Submitting a signed attestation

- Pharmacies should send their signed Attestation of Compliance to:

Health Insurance BC, Information Support,  
PO Box 9655 STN PROV GOVT  
Victoria BC V8W 9P2  
Fax: (250) 405-3599
- All other points of service should send their signed Attestation of Compliance to:

Health Data Access Services, Health Sector IM/IT Division, Ministry of Health,  
PO Box 9640  
STN PROV GOVT  
Victoria BC V8W 9P1  
Fax: (250) 952-1119
- Once you receive an e-mail confirmation from the Ministry, you may implement wireless access to PharmaNet.

### *Attestation term limits*

- Attestations must be renewed every two years. The ministry, however, reserves the right to require re-attestation at any time (e.g., following the publication of major changes to the wireless standards).

### *Failure to comply*

- Facilities that do not satisfy these requirements are not permitted to use wireless technology to access PharmaNet.
- Any facility that fails to comply with the above procedures in the deployment and use of wireless technology will have to terminate their wireless connection to PharmaNet and any other systems the Ministry specifies.

### *Tools and Resources*

- For assistance, contact the Ministry of Health Services HelpDesk at [Hlth.Helpdesk@gov.bc.ca](mailto:Hlth.Helpdesk@gov.bc.ca)

## 9.5 Patient Records

### General Policy Description

Patient information is stored on the PharmaNet Drug Information System (DIS) and PharmaCare Centralized Information System (PCIS).

### Policy Details

#### Patient Data Stored on PharmaNet

- When a prescription is dispensed, the following patient information is recorded:
  - name and address
  - date of birth
  - Personal Health Number
  - adverse drug reactions
  - drug allergies
  - any clinical conditions the patient may have
  - details of all prescription medications
- Up to the most recent 14 months of patient medication history is available online from PharmaNet.
- PharmaNet provides the pharmacist with a complete medication history for each patient, enabling more informed dispensing decisions. This history assists in detecting drug interactions and preventing adverse drug reactions.

#### Patient Record Access

- The details of all a patient's prescriptions stored on PharmaNet are available to any pharmacist in British Columbia and certain healthcare providers that have been granted access to PharmaNet, unless a patient **protective word** has been assigned restricting access.

*For more information on access to patient records by pharmacists, refer to Section [9.3](#).*

- A patient may choose to restrict access to their medication history by assigning a **protective word** to limit access to their records.

*For further information, refer to [Protective words](#).*

- The College of Pharmacists of British Columbia (CPBC) and a number of other provincial regulatory bodies have access to prescription data on PharmaNet, in order to **monitor** and regulate their respective professions.

*For more information refer to Section [9.3](#).*

#### Patient Requests to View their Own Data

- A patient may request a printed copy of their confidential and personal data (either the data stored on the local system, the data stored on PharmaNet, or both). A patient may make the request through any community pharmacy.

- A patient may also request a copy of their local system or PharmaNet patient record from a practitioner with Medical Practice Access to PharmaNet. The medical practice may print the local record but not the PharmaNet record which must be requested via PharmaNet.
- Although the local system record may be printed at the community pharmacy, the PharmaNet patient record may not be printed as College of Pharmacists of BC (CPBC) policy does not permit community pharmacies to print the PharmaNet patient record.
- Requests for PharmaNet data must be sent via PharmaNet to the CPBC using the Patient Access to Personal Data function (TPM transaction). The CPBC then mails the information directly to the patient.
- The CPBC requires pharmacists/medical practices to validate the patient's address and PHN on PharmaNet (TID transaction) and update the address (TPA transaction), if necessary, before requesting a mailing.
- The PharmaNet information sent to a patient includes:
  - patient demographic and clinical information
  - patient adverse reaction information
  - patient medication history for the last fourteen months
  - a log of all persons who have accessed the patient's information when no medication was dispensed.

*The medication history normally includes only medications from community and hospital out-patient pharmacies.*

>> See the CPBC [Obtaining Your PharmaNet Patient Record](#) website for further details.

>> Refer also to [Access by Patients](#).

## Procedures

### *Procedures for pharmacists and medical practices*

- Any B.C. resident may request a printed copy of their confidential and personal data, whether it be for information stored on a pharmacy's local system or the data stored on PharmaNet.
- The local patient record may be printed at the pharmacy.
- Patients can request a copy of their current PharmaNet patient record (past 14 months) through their community pharmacy at no charge.
- To process a patient's request for their PharmaNet record:
  1. Positively identify the patient.
 

>> Refer to [Positive Identification of Patients](#) for more details
  2. Validate the patient's address and PHN on PharmaNet (TID transaction) and update the address (TPA transaction), if necessary, before requesting a mailing.

*Validation of a patient's identification and address is mandated by the College of Pharmacists of BC to protect patient privacy and ensure the profile is mailed to the correct address.*



3. Send the request via PharmaNet using the Patient Access to Personal Data function (TPM).

*Depending on your pharmacy software, this function may be labelled in the menu as “Request Profile Mailing”. Please contact your software vendor if you need assistance with the procedure.*

- The request is automatically forwarded to the College of Pharmacists. The College will mail the information directly to the patient.

### *Tools and Resources*

- CPBC: [Obtaining Your PharmaNet Patient Record](#)

## 9.6 Protective Words

[June 1, 2015: Updated to reflect requirements of the Information Management Regulation]

### General Policy Description

A patient has the option of attaching a **protective word** to his or her PharmaNet patient record. The **protective word** limits access to the patient's record to only those pharmacists and authorized **health practitioners** to whom the patient provides the **protective word**.

### Policy Details

#### Protective Word Requirements

- The *Pharmaceutical Services Act* and its *Information Management Regulation* establish that at the request of an **adult** patient, a pharmacist must establish, delete or change the patient's PharmaNet **protective word**. Other requests (minors and requests for protective words on another patient's record) must be submitted in writing to Health Insurance BC.
- **Protective words** are not required but all patients must be informed of the **protective word** option.
- Patients must be informed of, and understand, the importance of keeping PharmaNet **protective words** confidential.
- Patients must be made aware that they cannot apply a protective word to only selected parts of their record (e.g., they cannot prevent users from viewing only specific prescriptions in their medication history). The patient's entire record is either restricted by the protective word or not.
- Patients must also be informed that the protective word may be overridden by authorized health care practitioners in an emergency situation where they are unable to provide it. See [Emergency Access if Protective Word Not Known](#).
- Hospital Access to PharmaNet, Emergency Department Access to PharmaNet, and Medical Practice Access to PharmaNet require compliance with the applicable PharmaNet Professional and Software Compliance Standards with regard to patient **protective words**. Refer to the [Compliance Standards Documentation for PharmaNet](#) website for further details.

#### Access to Protected PharmaNet Records

- After the **protective word** is set, it must be provided when:
  - accessing a patient's medication history
  - performing a Drug Use Evaluation (DUE)
  - dispensing a prescription
  - viewing any information about a patient's prescriptions (e.g., number of refills remaining, allergies recorded, prescription costs, etc.)
  - submitting a request on a patient's behalf to have their PharmaNet Medication History mailed to them (pharmacists only)
  - changing a **protective word** (pharmacists only)

- A patient’s physician must provide the **protective word** when calling the pharmacist for information contained on a patient medication history.
- The pharmacist may use the patient record on the pharmacy’s local system, when necessary, without a **protective word**.

### ***Emergency Access if Protective Word Not Known***

- Only an authorized regulatory body, such as the College of Pharmacists of BC, is able to enter a patient file without the **protective word** (for regulatory monitoring purposes only).
- In an emergency, however, if a patient unconscious or unable to provide their **protective word**, **authorized health care practitioners** can contact the PharmaNet HelpDesk at Health Insurance BC to have it removed if they determine access to the patient’s PharmaNet patient profile is necessary for safe and effective treatment.
- **Within a reasonable period of time after the protective word has been removed, the patient will be notified that it has been removed and that they must request a new word be applied.**

### ***Adding, removing or changing a protective word***

#### ***Who may request a protective word at a community pharmacy***

- Any person who is 19 or older can apply in person at a community pharmacy to update their PharmaNet record by adding, removing or changing a protective word.

*>> See [Procedures for Pharmacies below for details](#)*

- All other persons must apply in writing to Health Insurance BC. This includes:
  - minors (under 19) who wish to update their own PharmaNet record
  - persons (such as the guardian of a minor, or a person who is legally authorized to make decisions on another adult’s behalf) who wish to apply, remove or change a protective word on **another person’s** PharmaNet record

*>> Refer these patients to the [Protective word for a PharmaNet Record page on the PharmaCare website: www.gov.bc.ca/pharmanetaccess/protectiveword](#). It contains the necessary guidelines and application forms.*

#### ***Acceptable Proofs of Identity when Managing Patient Protective Words***

- The following identification requirements apply when managing patient protective words (i.e., when applying, removing or changing a protective word on the patient’s own PharmaNet record).
- Acceptable pieces of identification are set forth in the British Columbia Office of the Chief Information Officer’s [Evidence of Identity Standard](#); Section 3. The tables below summarize the acceptable pieces of identification.
- All proofs of identification must be **originals**, not photocopies.

<b>ACCEPTABLE PROOF OF IDENTITY</b>	
<b>Document Type</b>	<b>Requirements/Restrictions</b>
<b>Option 1</b>	
<ul style="list-style-type: none"> <li>BC Services Card with the patient's photo</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> <li>Must display a recent (within 5 years) photo</li> </ul>
<b>Option 2</b>	
<ul style="list-style-type: none"> <li>BC Services Card without photo</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> </ul>
<b>OR</b>	
<ul style="list-style-type: none"> <li>BC CareCard</li> </ul>	
<b>AND one of the following pieces of government-issued photo ID</b>	
<ul style="list-style-type: none"> <li>Canadian or U.S. Driver's Licence, Learner's Licence or Enhanced Driver's Licence</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> <li>Must display a recent (within 5 years) photo</li> </ul>
<ul style="list-style-type: none"> <li>BC Identification (BCID) card or Enhanced Identification Card</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> <li>Must display a recent (within 5 years) photo</li> </ul>
<ul style="list-style-type: none"> <li>Passport (Canadian or foreign)</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> </ul>
<ul style="list-style-type: none"> <li>Foreign Government Passport</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> </ul>
<ul style="list-style-type: none"> <li>U.S. Passport Card</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> </ul>
<ul style="list-style-type: none"> <li>Canadian Citizenship Card</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> <li>Must display a recent (within 5 years) photo</li> </ul>
<ul style="list-style-type: none"> <li>Canadian Permanent Resident Card</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> <li>Must display a recent (within 5 years) photo</li> </ul>
<ul style="list-style-type: none"> <li>Canadian Forces Identification</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> <li>Must display a recent (within 5 years) photo</li> </ul>
<ul style="list-style-type: none"> <li>Royal Canadian Mounted Police Identification</li> </ul>	<ul style="list-style-type: none"> <li>Must be valid (not expired)</li> <li>Must display a recent (within 5 years) photo</li> </ul>
<ul style="list-style-type: none"> <li>Secure Certificate of Indian Status Card</li> </ul>	<ul style="list-style-type: none"> <li>Must be new secure version issued after 2009. Certificate of Indian Status cards issued prior to 2009 are not accepted</li> <li>Must display a recent (within 5 years) photo</li> </ul>
<ul style="list-style-type: none"> <li>Any other credential or evidence approved by the Chief Information Officer for the Province of British Columbia</li> </ul>	<ul style="list-style-type: none"> <li>Where an individual is ineligible for one of the required credentials, additional credentials or evidence may be accepted where approved by the Chief Information for the Province of British Columbia as providing equivalent assurance.</li> </ul>

### **When names do not match**

- When the name on the patient's photo ID does not match the name in the PharmaNet record or on one or more other pieces of identification, the patient must provide additional documentation to establish a link between the two names.

ACCEPTABLE PROOF OF IDENTITY: Change of name	
Document Type	Requirements/Restrictions
Change of Name certificate	<ul style="list-style-type: none"> <li>• Must be issued by Canadian Province or Territory's Registrar of Vital Statistics</li> </ul>
Marriage Certificate, Certified Statement of Marriage, or Record of Marriage Form	<ul style="list-style-type: none"> <li>• Must be issued by Canadian Province or Territory's Registrar of Vital Statistics; or Clergy member, judge or justice of the peace that performed the marriage</li> <li>• Must be signed by the person who performed the marriage</li> <li>• Must contain the name of both spouses, the date of the marriage and licence number</li> </ul>
Any other credential or evidence approved by the Chief Information Officer for the Province of British Columbia	<ul style="list-style-type: none"> <li>• Where an individual is ineligible for one of the required credentials, additional credentials or evidence may be accepted where approved by the Chief Information for the Province of British Columbia as providing equivalent assurance.</li> </ul>

### ***Protective Word Removal***

- If an **adult** at a pharmacy has forgotten their **protective word**, a pharmacist can ask the [PharmaNet Help Desk](#) to remove it.
- If the patient's **protective word** is removed, **Health Insurance BC** will notify the patient in writing.
- The **protective word** can be changed only once in 24 hours but—should a patient lose or forget the **protective word**—the [PharmaNet Help Desk](#) may remove it.

### ***Creating a Protective Word***

- A patient must choose their own protective word which is then entered on PharmaNet by the pharmacist. A pharmacist cannot choose a protective word for a patient.
- The pharmacy must have policies and procedures in place to protect patient privacy when providing protective words (e.g., if the protective word cannot be spoken in a confidential manner, the pharmacy may provide pen and paper, disposing of the paper appropriately after use).
- The patient's protective word must contain:
  - 6 to 8 characters (no spaces allowed)
  - letters and numbers only (no special characters such as #,\ and &)
  - at least two letters (A...Z)
  - at least two numbers (0...9)

*Examples:* PA6729BC, 90PAMA17, FOTO2609

*Tips:* Patients should create a word that is easy for them to remember but hard for someone else to guess. They should NOT use their mother's maiden name, their birth date or their phone number. There is an increased likelihood of the information being discovered by an outside source and used to access PharmaNet information.

Patients should be encouraged to write down their protective word and store it in a safe place.

### **Storing and Sharing Patient *Protective Words***

- Protective words can be stored in the local system only with prior, explicit, consent from the patient.  
*The individual should be advised that all pharmacy staff will be able to view and use the protective word and will not need to ask the individual for it before accessing their PharmaNet record.*
- Protective words can be stored **only** in encrypted form in the local system's software. Consult your software documentation for directions.
- Protective words must not be stored on paper. If a patient writes out the protective word for you to enter into the system, you must either (a) return the paper to the patient for destruction or (b) immediately destroy it in a secure fashion.
- Protective words must not be shared with any other person or facility. They must not be made available to any other user across a shared network (e.g., pharmacy chain).
- You must remove a stored protective word from the local system immediately if the patient requests it.

#### ***Adding a **Protective Word** to a Patient's Own PharmaNet Record***

- The patient must be 19 or older and must provide adequate proofs of their identity before you can process their request.
  1. Review the patient's proofs of identity and confirm their age. If you have any concerns about these proofs, refer the patient to Health Insurance BC.
  2. Provide a private location in which the patient can provide you with a protective word that meets the rules above or have them write out the protective word so that it cannot be overheard.
  3. Attach the **protective word** to the patient's PharmaNet record using the Patient Keyword Maintenance (TCP) transaction.
  4. If applicable, destroy the paper bearing the protective word.
  5. Inform the patient that the change takes effect immediately.

#### ***Removing a **Protective Word** From a Patient's Own PharmaNet Record***

- The patient must be 19 or older and must provide adequate proofs of their identity before you can process their request.
  1. Review the patient's proofs of identity and confirm their age. If you have any concerns about these proofs, refer the patient to Health Insurance BC.
  2. Telephone the PharmaNet Help Desk at HIBC to remove the **protective word**.
  3. Inform the patient that the change takes effect immediately.

#### ***Changing a **Protective Word** on a Patient's Own PharmaNet Record***

- A patient can apply to change a **protective word** only once in a 24-hour period.
- The patient must be 19 or older and must provide adequate proofs of their identity before you can process their request.
- The patient must provide you with their current **protective word** for you to process the change using the Patient Keyword Maintenance (TCP) transaction.
- If they cannot remember the word, telephone the PharmaNet Help Desk at HIBC to have them remove the current **protective word**. Once it is removed, you can use the Patient Keyword Maintenance (TCP) transaction to add a new **protective word**.

#### ***When the patient can provide their current **protective word*****

1. Review the patient's proofs of identity and confirm their age. If you have any concerns about these proofs, refer the patient to Health Insurance BC.
2. Provide a private location in which the patient can provide you with a protective word that meets the rules above or have them write out the protective word so that it cannot be overheard.

3. Attach the **protective word** to the patient's PharmaNet record using the Patient Keyword Maintenance (TCP) transaction.
4. **If applicable, destroy the paper bearing the protective word.**
5. **Inform the patient that the change takes effect immediately.**

*When the patient cannot provide their current **protective word***

1. Review the patient's proofs of identity and confirm their age. If you have any concerns about these proofs, refer the patient to Health Insurance BC.
2. Telephone the PharmaNet Help Desk at HIBC to remove the patient's current **protective word**. Cite the type of identification provided.  
*The change will take effect immediately.*
3. Provide a private location in which the patient can provide you with a new protective word that meets the rules above or have them write out the protective word so that it cannot be overheard.
4. Attach the **protective word** to the patient's PharmaNet record using the Patient Keyword Maintenance (TCP) transaction.
5. **If applicable, destroy the paper bearing the protective word.**
6. **Inform the patient that the new protective word takes effect immediately.**

### *Tools and Resources*

- [Protective Word for a PharmaNet Record—Information for Patients](#)



## 9.7 PharmaNet Security

### General Policy Description

PharmaNet has many built-in security features to prevent unauthorized access to patient information—including data encryption, a “firewall” to prevent outside access to restricted files, and a system of tightly monitored access privileges.

PharmaNet was developed to address the diverse needs of individuals and organizations using it. Some users need “update” access to specific parts; others may require “read-only” access to specific information.

### Policy Details

#### Overview

- PharmaNet has several levels or layers of access security. Each user and organization has been granted the level of access required to perform their role in managing and using the system.
- Access to PharmaNet requires adherence to security requirements of the applicable PharmaNet Professional and Software Compliance Standards. Refer to the [Compliance Standards Documentation for PharmaNet](#) website for further details.
- The levels of security are as follows:
  - physical security
  - operating system security
  - network security
  - transaction security
  - screen security

#### Physical Security

- Physical security addresses physical access to the hardware components of PharmaNet. Physical security includes:
  - restricted access to premises in which the hardware resides
  - logging of all access to the PharmaNet equipment
  - inventory checking
  - security procedures for handling and storage of backup and storage media (tapes, discs, flash and hard drives, etc.).

#### Operating System Security

- Operating-system security regulates the security of the operating system, for example, by controlling user access and associated privileges, and by allocating PharmaNet system resources to allow PharmaNet to meet performance levels.
- Included in operating-system security are:
  - the assignment of required user IDs

- the establishment and administration of user password standards and policies
- the assignment of system resources to users with appropriate security clearance

### ***Network Security***

- Network security prevents access to the network by unauthorized users and unauthorized interception of data traveling to and from the network.
- PharmaNet's core system is behind a firewall on SPAN/BC, the provincial government's shared, province-wide data network. Most pharmacies are connected via the SPAN/BC network.
- Information or messages being transmitted are monitored and authenticated to ensure they are from authorized users. In addition, all personal information that may identify an individual is encrypted to prevent monitoring of the transaction data.

### ***Transaction Security***

- Transaction security grants or limits services to authorized individuals or groups. Each organization connected to PharmaNet is assigned a group of privileges based on the type of PharmaNet transactions it will use. This group of transactions represents the precise services that a specific organization is eligible to use.

### ***PharmaNet Screen Security***

- Screen security controls internal user or group access to specified PharmaNet database screens and the ability to perform specific functions on those screens.

*This description applies to internal screens that are part of PharmaNet, not the vendor-supplied screens that are located externally at pharmacies.*

- Based on each internal user's security profile, certain menu items, functions, screens, etc., may be made inaccessible. Some groups may be allowed to change or add information, other groups may be able only to read or view the information and others may have no access at all.