



# PharmaNet

Professional and Software Compliance Standards

## Volume 2 – Business Rules

### Hospital

Version 2.2

July 2009

<b>DOCUMENT MODIFICATION HISTORY</b>		
<b>VERSION</b>	<b>RELEASE DATE</b>	<b>DESCRIPTION</b>
1.0	December 2006	Initial release to vendors
1.1	February 2007	Revised format, clarified business rules
2.0	December 2007	1) Provide for centralized registration within implementer organizations by allowing multiple facilities on a single Confidentiality Undertaking, 2) remove requirement for written consent of the patient to access PharmaNet records, 3) strengthen privacy policy for access audits by providing for proactive access discrepancy alerting, 4) add new optional functionality to support prescriber identification and medication reconciliation
2.1	January 2009	Added language describing when a medication reconciliation report might be used.
2.2	July 2009	Medication reconciliation: Add distribution as a use, clarify report format and clarify usage. Include <i>Pharmacy Operations and Scheduling Act</i> and <i>Health Professions Act</i>

# CONTENTS

<b>1</b>	<b>GENERAL INFORMATION</b>	<b>4</b>
1.1	THE VOLUMES	4
1.2	THE AUDIENCE	5
1.3	THIS DOCUMENT	5
1.4	PHARMA <span>NET</span> OPERATION INFORMATION	6
<b>2</b>	<b>HOSPITAL</b>	<b>6</b>
2.1	IMPLEMENTATION REQUIREMENTS	7
2.1.1	<i>HA/Hospital Implementation Requirements</i>	7
2.1.1.1.	Health Authority Data Access Agreement	7
2.1.1.2.	Confidentiality Undertakings	8
2.1.1.3.	Patient Consent Requirements	9
2.1.2	<i>HA/DMHF Implementation Requirements</i>	10
2.1.2.1.	Health Authority Data Access Agreement	10
2.1.2.2.	Confidentiality Undertakings	10
2.1.2.3.	Patient Consent Requirements	12
2.1.3	<i>Business Overview</i>	12
2.1.4	<i>Business Rules</i>	14
2.1.5	<i>Software and Training</i>	17
2.2	PHARMA <span>NET</span> PARTICIPANT MESSAGING	17
2.2.1	<i>Business Overview</i>	17
2.2.2	<i>Business Rules</i>	18
2.3	MULTIPLE PHNS FOR PATIENT	18
2.3.1	<i>Business Overview</i>	18
2.3.2	<i>Business Rules</i>	18
2.4	PATIENT IDENTIFICATION - TID	18
2.4.1	<i>Business Overview</i>	18
2.4.2	<i>Business Rules</i>	19
2.5	PROCESS A PATIENT	19
2.5.1	<i>Business Overview</i>	19
2.5.2	<i>Business Rules</i>	19
2.6	PATIENT PROFILE REQUEST – TRP, TRR	19
2.6.1	<i>Business Overview</i>	19
2.6.2	<i>Business Rules</i>	20
2.7	PRESCRIBER IDENTIFICATION – TIP (OPTIONAL)	21
2.7.1	<i>Business Overview</i>	21
2.7.2	<i>Business Rules</i>	21
<b>3</b>	<b>DETECTION OF BROWSING</b>	<b>22</b>
3.1	PHARMA <span>NET</span> ACCESS DISCREPANCY REPORTING	22
3.1.1	<i>Business Overview</i>	22
3.1.2	<i>Business Rules</i>	23
3.2	REPORTING OF INAPPROPRIATE ACCESSES	24

# 1 GENERAL INFORMATION

The Professional and Software Compliance Standards Document for PharmaNet has been revised into volumes, divided by PharmaNet participant functionality requirements.

The 'library' approach provides more logical formatting while reducing redundancy and repetition.

There are common volumes required by all software developers and both business and technical volumes for the different functions. This enables software developers to download only the necessary volumes. The documentation is available on the Data Access Services web site. <http://www.healthservices.gov.bc.ca/das>

## 1.1 The Volumes

The 6-volume documentation set contains:

### Volume 1 – Introduction

Volume 1 introduces the reader to common development components, such as:

- Document Conventions and Structures
- Related Standard
- Contacts
- Support Responsibilities
- Compliance Evaluation Process
- Mandatory policies and procedures to ensure compliance with all standards.

### Volume 2 – Business Rules

Volume 2 has been further divided into separate documents for the functionality requirements of Hospital, Emergency Department (ED), Medical Practice (MP), and Pharmacy access.

This volume contains the *implementation requirements* and the *business rules* related to the use of the available transactions and the local system requirements.

### **Volume 3 – Technical Rules**

Volume 3 has been further divided into separate documents for the functionality requirements of Hospital, Emergency Department (ED), Medical Practice (MP), and Pharmacy access.

This volume contains the *general processing* and the *technical rules* related to the use of the available transactions and the *local system requirements*.

### **Volume 4 – HL7 Message Catalog**

Volume 4 identifies transaction details and message responses, such as:

- Network Transmissions and Responses
- Health Level 7 (HL7) Standards
- Message Formats and Data Definitions
- Input and Output Message Segments and Fields

### **Volume 5 – Security**

Volume 5 provides security objectives, requirements and guidelines and a framework for developing policies and implementing local security controls.

### **Volume 6 – Glossary**

Volume 6 lists a glossary of terms persistent through out PharmaNet.

## **1.2 The Audience**

The compliance standards documentation is intended for software developers, health care Providers, administrators and other health care professionals who share responsibility for implementing compliant software in their organization.

## **1.3 This Document**

This volume contains the business rules for using the PharmaNet transaction messages within hospital and Designated Mental Health Facility (DMHF) settings that are not part of the Emergency Department or pharmacy. For information on the transaction set supported in the Emergency Department or pharmacy refer to Volume 2 – Business Rules and Volume 3 – Technical Rules for those settings.

The PharmaNet transaction message set implemented within hospital and DMHF settings that are not part of the Emergency Department or pharmacy is a limited set of transactions for viewing purposes only.

For the purposes of this program, a DMHF is a designated facility, as defined in the *Mental Health Act*.

Read this volume in conjunction with Volume 3 – Technical Rules (Hospital).

## 1.4 PharmaNet Operation Information

Basic information regarding practitioners, prescribers and operators, must exist on PharmaNet before any message from a Provider will be accepted for processing. This information may be sent to PharmaNet in an electronic format by authorized individuals. Detailed specifications for this process are described in the document titled PharmaNet Practitioner and Operator Data Interface Specifications.

## 2 HOSPITAL

Hospital Access to PharmaNet is the expansion of authorized access to the existing PharmaNet data for physicians and pharmacists in hospitals and DMHFs. Expanding access to authorized care Providers is an eHealth goal and is a fundamental component of the vision for sharing health information. This new expanded service offering represents another step in the on-going expansion of authorized access to PharmaNet in clinical settings and is a key stepping stone to the provincial Electronic Health Record (EHR).

Hospital Access to PharmaNet will improve patient care by making the patient's medication history available to authorized individuals in hospitals and DMHFs in a timely and secure manner.

Access is only considered appropriate if:

1. there is a patient/Provider relationship;
2. access is associated with a hospital/DMHF patient encounter;
3. access occurs within the following window:
  - a) within 1 business day before or after a patient's hospital/DMHF clinic appointment; or
  - b) within 1 business day before a patient's admission to, or after discharge from, a hospital/DMHF;

4. the information retrieved is used only for the therapeutic treatment and care of patients as per the *Pharmacy Operations and Drug Scheduling (PODS) Act*;
5. the purpose and manner of access are consistent with Ministry of Health Services (MoH) standards
  - a) Data Access Agreement (DAA),
  - b) Undertaking of Confidentiality and Acknowledgement of Disclaimer, and
  - c) PharmaNet Application (PharmaNet Professional & Software Compliance Standards).
6. Access is made upon the request of a pharmacist or a physician or in accordance with the documented policies and procedures of the hospital/DMHF.

Access will be limited to 4 transactions for hospitals and DMHFs, as follows:

1. TID – View patient demographic information.
2. TRP – View full 14 month patient medication profile.
3. TRR – View the 15 most recent filled prescriptions.
4. TIP – View prescriber identification (optional transaction)

## **2.1 Implementation Requirements**

In order to obtain access to PharmaNet, hospitals/DMHFs must do the following:

### **2.1.1 HA/Hospital Implementation Requirements**

#### **2.1.1.1. Health Authority Data Access Agreement**

The DAA is an agreement between the MoH and the Health Authority responsible for the operation of the hospital. This Agreement is signed by the Chief Executive Officer (CEO), the Chief Operating Officer (COO), or their designate and submitted to the MoH. The DAA details such items as:

1. confidentiality;
2. permission to conduct spot audits / inspections by the PharmaNet compliance team;
3. administration and maintenance of operator IDs;
4. penalties for misuse of information;

5. problem escalation procedures (i.e., identification of key personnel); and
6. contact information.

#### **2.1.1.2. Confidentiality Undertakings**

##### **1. Professional Confidential Obligations of Physicians**

In addition to the provisions of the Hospital Access to PharmaNet, physicians are subject to the following confidentiality requirements:

Upon registration with the College of Physicians & Surgeons of British Columbia (CPSBC), every physician signs a document acknowledging receipt of a copy of the Canadian Medical Association (CMA) Code of Ethics adopted by the CPSBC and agreeing to abide by that Code of Ethics, and acknowledging the requirement to review and comply with the *Health Professions Act* and the Bylaws under the Act. These acknowledgements are retained at the CPSBC as a permanent record. CPSBC

Secondly, hospital staff privileges for physicians include maintenance of good standing and licensure with the CPSBC and include agreement to comply with hospital or regional medical staff bylaws and rules and regulations. Therefore, membership in the hospital medical staff also demands the need to maintain patient confidentiality. Documentation supporting the above must be retained by the hospital administration in a personal file for each physician and that document must be surrendered for review by the compliance audit team. CPSBC

##### **2. Undertaking to Complete Confidentiality Procedures for Hospital Access to PharmaNet**

Each hospital must sign an “Undertaking to Complete Confidentiality Procedures for Hospital Access to PharmaNet” which is forwarded to Data Access Services at the MoH, and a copy of the signed form must be retained on file.

The CEO, COO, or designate and the Chief of Medical Services must sign for the hospital(s) within their responsibility acknowledging:

- a) the responsibility of physicians and pharmacists working in the hospital(s);
- b) the agreement of the hospital(s) to ensure confidentiality provisions are in place regarding authorized persons with access to PharmaNet.

3. Undertaking of Confidentiality and Acknowledgement of Disclaimer by Physician for Hospital Access to PharmaNet

Hospital administration must have an “Undertaking of Confidentiality and Acknowledgement of Disclaimer by Physician for Hospital Access to PharmaNet” signed by each physician accessing confidential PharmaNet data from within the hospital. If audited these undertakings will be surrendered to and reviewed by the access audit team.

4. Undertaking of Confidentiality and Acknowledgement of Disclaimer by Authorized Person for Hospital Access to PharmaNet

Hospital administration must have an “Undertaking of Confidentiality and Acknowledgement of Disclaimer by Authorized Person for Hospital Access to PharmaNet” for each person other than physicians and pharmacists accessing confidential PharmaNet data from within the hospital. If audited these undertakings will be surrendered to and reviewed by the access audit team.

### 2.1.1.3. Patient Consent Requirements

Written consent from the patient is **not** required prior to access of the patient’s PharmaNet medication profile.

To ensure patients know that their PharmaNet profile may be accessed, a hospital must:

1. Post a poster in clear view of patients presenting to the hospital. This poster must indicate that their medication information may be accessed and provide a contact for further information. Recommended content for the poster can be obtained from the Data Access Services website:  
<http://www.healthservices.gov.bc.ca/das/index.html>.
2. Have available an information sheet with more detail about PharmaNet and the access to patient records. An original copy of the information sheet can be obtained from the Data Access Services website:  
<http://www.healthservices.gov.bc.ca/das/index.html>.
3. Identify a hospital contact that may be consulted by a patient who requires further discussion or answers to questions.

Physicians are advised that where the care provided is neither urgent nor emergent, consent from their patients is required to access PharmaNet. Such consent may be formally documented by the retention of a signed consent, or it may be recorded in the chart as part of the informed consent discussion with the patient. If physicians are unable to obtain patient consent to access PharmaNet

for elective care, they may decline to provide treatment to the patient if, in their judgment, the absence of such access may compromise the care they provide. Where a patient is seen repeatedly by the same physician, the original consent remains valid (unless withdrawn) and the consent process and documentation does not have to be repeated for each interaction. CPSBC

## **2.1.2 HA/DMHF Implementation Requirements**

### **2.1.2.1. Health Authority Data Access Agreement**

Only DMHFs operating under the jurisdiction of a Health Authority can obtain access to PharmaNet through this Agreement.

Before DMHFs operating under the jurisdiction of the Ministry of Children and Family Development can obtain access to PharmaNet, the Ministry of Children and Family Development must sign a DAA with the MoH.

The DAA is an agreement between the MoH and the Authority responsible for the operation of the DMHF. This Agreement is signed by the CEO, COO or designate and submitted to the MoH. The DAA details such items as:

1. confidentiality;
2. permission to conduct spot audit / inspections by the PharmaNet compliance team;
3. administration and maintenance of operator IDs;
4. penalties for misuse of information;
5. problem escalation procedures (i.e., identification of key personnel): and
6. contact information.

### **2.1.2.2. Confidentiality Undertakings**

1. Professional Confidential Obligations of Physicians

In addition to the provisions of the Hospital Access to PharmaNet, physicians are subject to the following confidentiality requirements:

Upon registration with the College of Physicians & Surgeons of British Columbia (CPSBC), every physician signs a document acknowledging receipt of a copy of the CMA Code of Ethics adopted by the CPSBC and agreeing to abide by that Code of Ethics, and acknowledging the requirement to review and comply with the *Health Professions Act* and the

Rules made under the *Health Professions Act*. These acknowledgements are retained at the CPSBC as a permanent record. CPSBC

Secondly, hospital staff privileges for physicians include maintenance of good standing and licensure with the CPSBC and include agreement to comply with hospital or regional medical staff bylaws and rules and regulations. Therefore, membership in the hospital medical staff also demands the need to maintain patient confidentiality. Documentation supporting the above must be retained by the hospital administration in a personal file for each physician and that document must be surrendered for review by the compliance audit team. CPSBC

2. Undertaking to Complete Confidentiality Procedures for Designated Mental Health Facility Access to PharmaNet

Each DMHF must sign an “Undertaking to Complete Confidentiality Procedures for Designated Mental Health Facility Access to PharmaNet” which is forwarded to Data Access Services at the MoH, and a copy of the signed form must be retained on file.

The CEO, COO or designate and the Director of the DMHF(s) must sign for the DMFH(s) within their responsibility acknowledging:

- a) the responsibility of physicians and pharmacists working in the DMHF(s);
- b) the agreement of the DMHF(s) to ensure confidentiality provisions are in place regarding DMHF authorized persons with access to PharmaNet.

3. Undertakings of Confidentiality and Acknowledgements of Disclaimer by Physician for Designated Mental Health Facility Access to PharmaNet

DMHF administration must have an “Undertaking of Confidentiality and Acknowledgement of Disclaimer by Physician for Designated Mental Health Facility Access to PharmaNet” signed by each physician accessing confidential PharmaNet data from within the DMHF. If audited these undertakings will be surrendered to and reviewed by the access audit team.

4. Undertakings of Confidentiality and Acknowledgements of Disclaimer by Authorized Person for Designated Mental Health Access to PharmaNet

DMHF administration must have an “Undertaking of Confidentiality and Acknowledgement of Disclaimer by Authorized Person for Designated Mental Health Facility Access to PharmaNet” for each person other than physicians and pharmacists accessing confidential PharmaNet data from

within the DMHF. If audited these undertakings will be surrendered to and reviewed by the ministry access audit team.

### **2.1.2.3. Patient Consent Requirements**

Written consent from the patient is **not** required prior to access of the patient's PharmaNet medication profile.

To ensure patients know their PharmaNet profile may be accessed, a DMHF must:

1. Post a poster in clear view of patients presenting to the facility. This poster must indicate that their medication information may be accessed and provide a contact for further information. Recommended content for the poster can be obtained from the Data Access Services website:  
<http://www.healthservices.gov.bc.ca/das/index.html>.
2. Have available an information sheet with more detail about PharmaNet and the access to patient records. An original copy of the information sheet can be obtained from the Data Access Services website:  
<http://www.healthservices.gov.bc.ca/das/index.html>.
3. Identify a facility contact that may be consulted by a patient who requires further discussion or answers to questions.

Physicians are advised that where the care provided is neither urgent nor emergent, consent from their patients is required to access PharmaNet. Such consent may be formally documented by the retention of a signed consent, or it may be recorded in the chart as part of the informed consent discussion with the patient. If physicians are unable to obtain patient consent to access PharmaNet for elective care, they may decline to provide treatment to the patient if, in their judgment, the absence of such access may compromise the care they provide. Where a patient is seen repeatedly by the same physician, the original consent remains valid (unless withdrawn) and the consent process and documentation does not have to be repeated for each interaction. CPSBC

### **2.1.3 Business Overview**

The Health Authorities have been asking for access to PharmaNet in hospitals for some time. The urgency of the requirement was documented in the spring of 2006 when Health Authority clinical representatives made an urgent appeal for broader access to PharmaNet throughout the hospital. Delivery of this service was their highest priority requirement for patient safety.

As a result of additional investigation into the requirement to broaden PharmaNet access to hospitals, it was determined that access to PharmaNet for DMHFs

would also provide patient safety benefits. The recent coroner's inquest into the 2005 death of a Victoria psychiatric patient underscores the need for hospital and DMHF access to PharmaNet. The coroner's jury recommended that a patient's PharmaNet record be accessed as part of the admission process.

PODSA and its regulations permit access to PharmaNet by physicians, pharmacists and other authorized persons "for the purpose of providing therapeutic treatment or care to patients".

Physicians, pharmacists and authorized persons in a hospital and DMHF have a great need for PharmaNet access, in areas other than Emergency Departments and pharmacy. For example, general practitioners and specialists assessing and treating patients in a hospital/DMHF ward, urgent care centre, cardiac care clinic, renal clinic or pre-admission clinic would consider access to PharmaNet invaluable. Most of the patients are seen on an inpatient basis; however, some of the clinics operate both an inpatient and outpatient service for patients.

A BC Personal Health Number (PHN) is necessary in order to retrieve a patient's medication profile. Most people who have come in contact with publicly funded health care services in BC will have been assigned a PHN, even if they are not a BC resident. A PHN does not imply Medical Services Plan (MSP) eligibility or provide any indication of an individual's benefit status. The PHN has been identified as a provincial standard for the identification of clients of the health care system.

Hospital Access to PharmaNet will occur by one of two methods. The business rules for each may differ:

#### Stand-alone system

This is a software product which is not integrated with hospital/DMHF operations and has been built and installed with the key focus of providing PharmaNet access. Typically, the database of information would only be accessible to an authorized user of the stand-alone system.

#### Integrated system

This is a software product where PharmaNet access is one of many functions provided. The software is used to meet many other requirements of the hospital/DMHF. In this case, the hospital/DMHF's database would be on a central server accessible to authorized users throughout the hospital/DMHF. All patient information must be treated with the same high degree of confidentiality as any other patient or hospital/DMHF information.

#### 2.1.4 Business Rules

1. All staff in the hospital or designated mental health facility must be fully aware that access to sensitive information is under the control of the:
  - a) Physician requesting the patient's profile in the hospital or designated mental health facility. CPSBC; or
  - b) Pharmacist requesting the patient's profile in the hospital or designated mental health facility. CPBC
2. Computer screens and printers must be located so as to prevent viewing of information by the public or by unauthorized staff.
3. Under PODSA and its regulations the following persons are designated as having authority to access patient record information on the PharmaNet system for the purpose of providing therapeutic treatment or care to hospital/DMHF patients:
  - a) a medical practitioner who is a registrant of the College of Physicians and Surgeons of British Columbia and who is in good standing with the College;
  - b) a pharmacist who is a registrant of the College of Pharmacists of British Columbia and who is in good standing with the College; and
  - c) any other person authorized by a medical practitioner to have access:
    - i. under the direct supervision of the medical practitioner; and
    - ii. in the course of carrying out the person's employment or other duties in the hospital/DMHF.
4. It is the decision of each hospital/DMHF (Chief of Medical Services of a hospital or the Director of a DMHF) in consultation with hospital/DMHF administration on how to implement access to the PharmaNet data. Policies and procedures regarding this access may differ from hospital/DMHF to hospital/DMHF. A policies and procedures template along with supporting forms is available on the Data Access Services web site. <http://www.healthservices.gov.bc.ca/das>. Policies and procedures must be completed and retained by hospital/DMHF administration. The exact text contained in the policies, procedures and supporting forms must be retained except where options or variable wording is noted. The completed policies and procedures must be made available at the request of the access audit team.

5. The two measures in place today to ensure compliance with PharmaNet standards will continue as authorized by the DAA between the MoH and the appropriate hospital/DMHF governing authority. These measures are:
  - a) Compliance evaluation of new software products or new releases of software products which access PharmaNet; and
  - b) Random unannounced spot audits and inspections.

These measures will continue to be performed by a joint team of representatives from the PharmaNet technical administrators (technical) and the CPBC (use of the drug profile).

6. Hospital Access to PharmaNet includes Diagnostic and Treatment Centers.
7. Access to PharmaNet must be restricted to those physicians, pharmacists, and authorized persons who are authorized to access PharmaNet data.
8. Terminals and printers must be in a protected area in the hospital/DMHF, under the control of and approved by hospital/DMHF administration.
9. The use of remote access software to access the personal information in PharmaNet is only permitted by Software Support Organizations (SSO) who are accessing the information from within Canada and are accessing it for the sole purpose of supporting the software.
10. Access to PharmaNet must employ HNSecure which meets the security, privacy and confidentiality needs where the transmission of data will occur over public, shared telecommunications lines (i.e., the Internet). The MoH has adopted HNSecure as the security infrastructure for message-based communications. It addresses concerns related to unauthorized alteration of messages, confirmation of sender and receiver and 'eavesdropping'.
11. Access to PharmaNet using wireless technology must satisfy the following:
  - a) The use of any privately owned wireless devices, such as personal digital assistants, laptops, or cell phones, to access PharmaNet is not permitted;
  - b) Only Health Authority managed devices may be used to access PharmaNet;
  - c) The use of wireless technology such as a wireless router or local area network must meet the controls as specified in Volume 3 - Technical Rules (Hospital);
  - d) Before deploying the use of wireless technology such as a wireless router or local area network, a Security Threat Risk Assessment

(STRA) must be performed to demonstrate that the wireless communications meets the controls as specified in Volume 3 - Technical Rules (Hospital). This STRA must be approved by the Ministry as part of the compliance review of the Health Authority security practices for HAP. This STRA must be kept current, on file and provided for review by the audit/inspection team. Any previous versions must be kept for a minimum period of two years and provided for review by the audit/inspection team.

12. The CPSBC identification number of the responsible physician or the CPBC registration number of the pharmacist working in the hospital/DMHF must be included with every message sent to PharmaNet.
13. Hospital/DMHF access to PharmaNet data must only take place
  - a) within 1 business day before or after a patient's hospital/DMHF clinic appointment; or
  - b) within 1 business day before a patient's admission to, or after discharge from, a hospital/DMHF.
14. SSOs must train personnel selected by the hospital/DMHF administrator, authorized physician or authorized pharmacist. The hospital/DMHF administrator authorized physician or authorized pharmacist must ensure that all authorized Providers receive training on business rules, software functions and features, and policies and procedures developed for hospital/DMHF access to PharmaNet.
15. Some patients may have assigned keywords to protect their medication profiles. The patient must supply the keyword to allow an authorized health care professional to access their medication profile. If the patient supplies a keyword, it must be erased from all hospital/DMHF records relating to them, when they are no longer receiving care or treatment from the hospital/DMHF.
16. Indirect Collection

A Provider or staff member may also collect personal information from another individual or organization if the physician has reasonable grounds to believe that indirect collection is necessary for the safe and effective treatment of the patient (including urgent and immediate circumstances, or where the patient is incapable of providing the information). CPSBC

Reasonable grounds are based on the best judgement of the physician at the time of treatment.

Indirect collection would be accomplished by the physician working in the hospital/DMHF or a nurse or clerk, authorized by the physician, contacting the PharmaNet Help Desk to have the patient's keyword removed. The physician who asked to have the keyword removed must notify the patient by secure means of this action within a reasonable time after the keyword was removed and before the patient is discharged from the hospital. This will ensure that the patient is aware that their keyword has been removed and that they will need to re-establish a keyword if required.

When a keyword removal is requested the PharmaNet Help Desk will request and record:

- a) The PHN and name of the patient;
- b) The Hospital ID of the patient cited;
- c) The CPSBC ID and name of the attending physician; and
- d) The name of the individual calling on behalf of the physician.

The Help Desk will also be responsible for notifying the CPBC that the keyword has been removed.

The CPBC will notify the patient, in writing at their last known address, that their keyword was removed as a result of the hospital/DMHF visit.

### **2.1.5 Software and Training**

1. Hospitals/DMHFs must install PharmaNet compliant software.
2. Physicians, pharmacists and / or designated support staff must receive training/education on use of the local software from the SSO supplying the software.

## **2.2 PharmaNet Participant Messaging**

### **2.2.1 Business Overview**

This function (fan out) is used to transmit urgent messages to all Providers or to a specified list (e.g., locations within a geographic region, specific software users or specific agencies).

When a transaction is processed, PharmaNet checks to determine if any message(s) are pending for that location. If there are, these pending message(s) are added to the transaction response message. Once the message is returned

to the location, the message status changes to 'sent'. Only one copy of the message is sent to each location.

### **2.2.2 Business Rules**

1. It is the responsibility of the Provider to ensure all appropriate personnel are made aware of the contents of the message.
2. On occasion important messages may be issued to all or selected participants. PharmaNet distributes fan out messages by attaching them to responses to certain information requests. The MoH recommends that participants issue at least one information request message each work cycle to ensure that any pending fan out messages are received.

## **2.3 Multiple PHNs for Patient**

### **2.3.1 Business Overview**

In some cases, a PHN may be assigned to a patient when one already exists for that patient. These duplicate PHNs are then merged on the Client Registry System (CRS) into a single PHN record. If a PHN has been merged with another PHN(s), PharmaNet will return the merged PHN.

### **2.3.2 Business Rules**

1. When the Provider is notified, via a message returned by PharmaNet, that a PHN is merged, the Provider must perform a TID and verify the patient demographics on PharmaNet against those on the local system.
2. If the information returned by PharmaNet on the TID appears correct, the Provider must update the local system with the merged PHN.
3. If the merge appears to have been done incorrectly, the Provider must contact the PharmaNet Help Desk to request correction or un-merge.

## **2.4 Patient Identification - TID**

### **2.4.1 Business Overview**

This inquiry is used to verify patient demographic information when the PHN is known.

The inquiry requires a PHN to be entered and will return demographic information associated with that patient record. The Provider may then confirm this demographic information with the patient to ensure the information on PharmaNet is correct.

#### **2.4.2 Business Rules**

None

### **2.5 Process a Patient**

#### **2.5.1 Business Overview**

Prior to treating a patient, the physician or pharmacist working in the hospital/DMHF may review the patient's medication profile in order to identify potential contraindications to treatment in the hospital/DMHF or to identify possible causes for the patient's symptoms.

#### **2.5.2 Business Rules**

None

### **2.6 Patient Profile Request – TRP, TRR**

#### **2.6.1 Business Overview**

The patient medication profile is that portion of the patient record containing the medication history, clinical condition, adverse reactions and associated comments recorded for the patient.

The patient medication profile request allows the Provider to review all dispensed medications and associated comments for a patient during the past 14 months, including all adverse reactions, clinical conditions, and associated comments, from all PharmaNet connected BC pharmacies. Profiles are available in the following formats:

Retrieve Full Profile – TRP

Returns prescriptions dispensed or reversed for reasons other than data entry errors during the last 14 months.

Retrieve Most Recent Only – TRR

Returns the most recent 15 prescriptions dispensed or reversed for reasons other than data entry errors. This is the most convenient format to use for an initial inquiry.

### 2.6.2 Business Rules

1. To ensure that the data is accurate for the next Provider, if an error is discovered in the medication profile, the physician or designate should advise the CPBC by secure means. This notification should provide the PHN, name of the patient and a brief description of the discrepancy. CPBC
2. To ensure that the data is accurate for the next Provider, if an error is discovered in the medication profile, the pharmacist or designate should advise the CPBC by secure means. This notification should provide the PHN, name of the patient and a brief description of the discrepancy. CPBC
3. The patient medication profile may be displayed, printed or distributed by a medical practitioner or pharmacist working in the hospital/DMHF, or by an authorized member of hospital/DMHF staff who is working under the supervision of a medical practitioner, only on the following conditions:
  - a) The purpose of displaying, printing and/or distributing the medication profile is to enhance the therapeutic care or treatment of the patient;
  - b) The medication profile is only used for review by a medical practitioner or pharmacist in a hospital, Designated Mental Health Facility, Emergency Department, Medical Practice, or Pharmacy; and
  - c) The printed or distributed copy or image of the medication profile must either be maintained on the patient's medical chart or record, or it must be appropriately destroyed.
4. Retention of an electronic 'picture' (a single, electronic image) of the medication profile is permitted. Access to this electronic 'picture' could eliminate the need for a printed medication profile, but is subject to all the same confidentiality, security and retention requirements of a printed profile. The electronic 'picture' must be stored as a single image that cannot be modified or downloaded. The electronic 'picture' must be time stamped and the local system must log all accesses to the electronic copy. A report showing all accesses must be made available upon demand by either the Audit Team or the patient.
5. If the patient medication profile is printed or distributed, only one of the following two report formats may be used (see Volume 3 – Technical Rules (Hospital) for more details on display and print standards):
  - a) Medication Profile Report format;

- b) Medication Reconciliation Report format.
6. On discharge, printed copies of the medication profile may be given to the patient in unusual circumstances (i.e., the printed profile will be delivered to the patient by the family doctor).

In most cases the patient should be encouraged to request a copy through any community pharmacy in the province. The printing of these profiles for use by patients will remain a centralized function (by the CPBC) as this provides:

- a) consistency of content and format;
- b) accuracy of information;
- c) additional information not available elsewhere such as a log of all accesses; and
- d) fulfillment of the positive ID requirement.

## **2.7 Prescriber Identification – TIP (optional)**

### **2.7.1 Business Overview**

This optional function may be used to obtain information on a Provider (e.g., physician, pharmacist, podiatrist, dentist, veterinarian, etc.) by either searching by name or by the unique identification number assigned by the appropriate regulatory body. Please note that MSP billing numbers are not used to identify Providers anywhere in PharmaNet.

### **2.7.2 Business Rules**

1. In some cases the PharmaNet Help Desk staff will be able to add Provider information to PharmaNet. Prior to adding this information, the PharmaNet Help Desk staff will validate the Provider using information from the appropriate provincial regulatory authority. The CPBC and CPSBC transmit electronic uploads to PharmaNet on a daily basis with the information regarding their members.
2. PharmaNet uses the Provider ID number and Provider reference number for Providers as assigned by the appropriate regulatory body.
3. As the Provider's name on PharmaNet could be different than the name commonly used by the practitioner, we recommend the following procedure when using TIP to search for a Provider on PharmaNet:

- a) First, use TIP to search using the Provider's family name only (i.e., no first name used); and,
- b) If too many matches are returned add the Provider's first initial of the first name and submit another TIP search.

### **3 DETECTION OF BROWSING**

In accordance with the terms of the DAA, the Health Authority or the Ministry of Children and Family Development is required to investigate all instances of the following that occur in facilities which fall within their respective responsibilities:

1. Unauthorized access;
2. Misuse of information; and
3. Breaches of confidentiality.

#### **3.1 PharmaNet Access Discrepancy Reporting**

##### **3.1.1 Business Overview**

The purpose of PharmaNet access discrepancy reporting is to identify apparent unauthorized accesses of PharmaNet data that may constitute browsing. Access to PharmaNet is considered appropriate if:

1. There is a patient/Provider relationship;
2. The access is associated with a hospital/DMHF encounter or visit;
3. access occurs within the following window:
  - a) within 1 business day before or after a patient's hospital/DMHF clinic appointment; or
  - b) within 1 business day before a patient's admission to, or after discharge from, a hospital/DMHF;
4. The information retrieved is used only for the care and treatment of the patient as per PODSA;
5. The purpose and manner of the access is consistent with the DAA, Undertaking of Confidentiality and Acknowledgement of Disclaimer (Physician or Authorized Person) and the Professional and Software Compliance documents.

6. The access is made upon the request of a pharmacist or a physician or in accordance with the documented policies and procedures of the hospital/DMHF.

Potential inappropriate accesses to PharmaNet must be identified and investigated and, if deemed inappropriate, reported and escalated as described in Section 3.2 Reporting of Inappropriate Accesses.

### **3.1.2 Business Rules**

1. PharmaNet access discrepancy reporting must:

- a) Identify all exceptions to the following minimum requirements for appropriate access:
    - i. the access must occur within 1 business day before or after a patient's hospital/DMHF clinic appointment; or  
  
within 1 business day before a patient's admission to, or after discharge from, a hospital/DMHF;
    - ii. the access must be by an authorized physician, pharmacist or their authorized person; and
    - iii. the access must be in accordance with documented hospital/DMHF policy.
  - b) To the extent possible, meet the following best practice criteria for identifying potential inappropriate accesses by identifying accesses where:
    - i. the user's last name matches to the patient's current, maiden or other 'alias' last name;
    - ii. the user's last name matches with the last name of anyone listed in the patient's file as a person to notify or family member/next of kin or guarantor;
    - iii. the user's phone number and/or address and/or postal code are the same as the patient's and/or anyone listed in the patient's file;
    - iv. the patient's last name matches against employee's names (i.e. if employee Joe Smith looks up patient records for Jane Doe and there is a Jason Doe working in the facility, the access gets reported as a potential breach); and
    - v. the access is to a patient who is a public figure or VIP.
2. The specific design of PharmaNet access discrepancy reporting is subject to the level of system integration and the infrastructure capacity available. PharmaNet access discrepancy reporting can be produced using one of the following two methods:

- a) **PharmaNet Access Reconciliation:** where access is implemented using a standalone system it is expected that the access discrepancy reporting process will include a reconciliation of the point of service PharmaNet transaction log with patient registration or clinic appointment information in order to meet minimum reporting requirements as specified in 1a above; Or,
- b) where PharmaNet access is integrated with clinical information systems, PharmaNet discrepancy reporting can be accomplished using a combination of:
  - i. Level 1 – near real time notifications; and
  - ii. Level 2 – regularly scheduled automated reports from the PharmaNet access log data that typically reveal exceptions and patterns over multiple accesses.

Note that regardless of the PharmaNet access discrepancy reporting method used, all exceptions to the minimum requirements for appropriate access as described in item 1a above must be reported.

- 3. The PharmaNet access discrepancy reporting must be performed by a designated individual at least weekly. This may be the Chief of Medical Services for a hospital or the Director of a DMHF, an RN, or a hospital/DMHF FOI administrator, etc.
- 4. All apparent inappropriate accesses must be investigated. These may be the result of errors in data entry (i.e. searching 'Block' versus 'Black'), problems related to accurate patient identification, etc. The outcome of the investigation of an apparent inappropriate access must be documented and maintained along with the PharmaNet access discrepancy reports for a period of two years for review by the audit/inspection team.
- 5. PharmaNet access discrepancy reporting must be documented as part of the facility's Hospital Access to PharmaNet policies and procedures. These policies and procedures must demonstrate that reasonable due diligence has been performed to ensure the protection of privacy to the level expected by established privacy best practices.
- 6. Apparent inappropriate accesses that cannot be resolved must be reported/escalated as described in the next section.

### **3.2 Reporting of Inappropriate Accesses**

The responsibility for authorizing access to PharmaNet lies with the pharmacist or the physician working in the hospital/DMHF or in accordance with the documented policies and procedures of the hospital/DMHF.

All apparent inappropriate accesses that have not been resolved, as described above must be reported using the Health Authority or Ministry of Children and Family Development's Freedom of Information privacy breach procedures, depending on the authority governing the facility.

Records related to the investigation, reporting, escalation and penalization of PharmaNet privacy breaches must be maintained for a period of two years for review by the audit/inspection team.