# Table of Contents

1. Introduction ........................................................................................................... 3
2. Definitions ............................................................................................................. 4
3. Medical Device Distributor Access to PharmaNet ................................................ 5
4. Confidentiality Undertakings ................................................................................. 5
5. Training ................................................................................................................ 6
6. Responsibilities of the Manager ............................................................................ 6
7. Individuals Authorized to Access PharmaNet ....................................................... 7
8. Security ................................................................................................................ 8
9. Patient Records ..................................................................................................... 9
10. Patient Profiles .................................................................................................... 9
11. Claims Access Discrepancy Reporting ............................................................. 10
12. PharmaNet Access Audits ................................................................................. 10
13. Help Procedures ............................................................................................... 11
14. Downtime ........................................................................................................... 11
15. Patient Keyword ................................................................................................. 11
16. Miscellaneous ..................................................................................................... 11

Appendix A – Acknowledgement of Completion of Confidentiality Procedures for Medical Device Distributor Claims Access to PharmaNet ........................................ 12
Appendix B – Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Manager ...................................................................................... 14
Appendix C – Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Authorized Person ................................................................... 16
Appendix D – Medical Device Distributor – Software Vendor PharmaNet Third Party Confidentiality Undertaking .................................................................................... 18
Appendix E – Patient Identification ......................................................................... 19
Appendix F – Privacy Breach Response Procedures .................................................. 20
Medical Device Distributor
Claims Access to PharmaNet
Policies & Procedures

1. Introduction

This document establishes the policies and procedures relevant for Medical Device Distributor claims access to PharmaNet. It sets out the security and confidentiality standards that Medical Device Distributors must comply with in order to establish and maintain connectivity with PharmaNet.

The PharmaNet transaction message set implemented within the Medical Device Distributor setting is a limited set of transactions for PharmaCare Claims Purposes Access only, specifically:

1. Adjudicate claims – submission, reversal and re-transmission of a claim;
2. View own previous transactions;
3. View store totals – There are four different transactions available:
   a) Daily Totals provides total number of claims, same day reversals, and prior day reversals for a particular adjudication date;
   b) Claim Details provides a list of claims processed for a particular day as well as the amount paid by PharmaCare for each of them;
   c) Same Day Reversals provides a list of claims that were reversed on the same day for a particular day, as well as the dollar amount of each reversed claim;
   d) Prior Day Reversals provides a list of claims that were reversed from a previous day, as well as the dollar amount of each reversed claim; and
4. Input a Personal Health Number (PHN) and verify the claim will be submitted for the correct person.

Medical Device Distributors will not be able to perform the following tasks:

1. Update personal information such as keywords, address, profile information;
2. Create PHNs;
3. View prescriber information;
4. Enter in a partial name and retrieve a list of similar names;
5. View First Data Bank drug monograph information;
6. Modify or view eligibility records (Software Support Organizations are not able to submit this transaction); or
7. Request that a patient’s profile be mailed to them.

Failure to comply with any of the policies and procedures set out in this document may result, at the option of the Ministry of Health Services (MOHS), in a refusal to allow the Medical Device Distributor connectivity with PharmaNet, or in the disconnection of the Medical Device Distributor from PharmaNet.
2. Definitions

In this document:

“Authorized Person” means an employee of the Medical Device Distributor who is working at the Distributor Site and who is authorized, by the Manager, to have PharmaCare Claims Purposes Access to PharmaNet in the course of carrying out that person’s employment duties;

“Distributor Site” means the physical premises at which the Medical Device Distributor accesses PharmaNet claims;

“Manager” means the individual at the Distributor Site with supervisory responsibility in relation to:
   a) the operation of the Distributor Site; and
   b) the employees of the Medical Device Distributor working at the Distributor Site;

“Patient Record” means a record of all medical devices and/or supplies dispensed to a particular patient, as well as information pertaining to that patient; and

“PharmaCare Claims Purposes Access” means access to PharmaNet for the purpose of submitting a PharmaCare claim to the British Columbia PharmaCare program or for the purpose of receiving confirmation or denial of payment of a PharmaCare claim from the British Columbia PharmaCare program.
3. Medical Device Distributor Access to PharmaNet

Medical Device Distributor (MDD) access to PharmaNet is only permitted if:

a) there is a patient/MDD relationship;
b) access is associated with the provision of one or more medical devices and/or associated supplies to the patient;
c) PharmaCare Claims Purposes Access is the sole type of access to PharmaNet by the MDD;
d) access occurs on the day the claim is entered onto PharmaNet;
e) information retrieved from PharmaNet is used only for the purpose as set out in b) above;
f) the access is by the Manager, or by an Authorized Person supervised by the Manager; and
g) the purpose and manner of access are consistent with this Policies and Procedures document.

4. Confidentiality Undertakings

Prior to being connected to PharmaNet, the Medical Device Distributor (MDD) must arrange for the following documents to be signed, and, where required, provided to the Ministry of Health Services (MOHS).

Acknowledgement of Completion of Confidentiality Procedures

An "Acknowledgement of Completion of Confidentiality Procedures for Medical Device Distributor Claims Access to PharmaNet" (URL: https://www.health.gov.bc.ca/exforms/das/4551fil.pdf) must be signed by the Chief Executive Officer or other senior officer of the MDD, by the Manager of the Distributor Site, and by two witnesses. The signed and witnessed original must be provided to Data Access Services at the MOHS. A signed copy of the form must be retained on file at the Distributor Site. By signing, the Chief Executive Officer or other senior officer and the Manager of the Distributor Site are acknowledging the MDD’s agreement to ensure confidentiality provisions are in place regarding MDD access to PharmaNet.

Confidentiality Undertaking by Manager of Medical Device Distributor Site

A "Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Manager" (URL: https://www.health.gov.bc.ca/exforms/das/4549fil.pdf) must be signed by the Manager and one witness. A signed copy of the form must be retained on file at the Distributor Site. The Manager is responsible for all activities undertaken at the Distributor Site in relation to PharmaNet.
Confidentiality Undertaking by Authorized Person

Prior to any Authorized Person accessing PharmaNet, that Authorized Person must sign a "Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Authorized Person" (URL: https://www.health.gov.bc.ca/exforms/das/4550fil.pdf). The form must also be signed by the manager who witnesses the staff member’s signature. Each signed form must be retained on file at the Distributor Site. All Authorized Persons must be fully aware that PharmaNet access is under the control of the Manager.

Identify the location where the confidentiality undertakings and the “Acknowledgement of Completion of Confidentiality Procedures” will be stored:

5. Training

An approved Software Support Organization (“SSO”) must train the Manager and all Authorized Persons. The Manager must ensure that Authorized Persons receive training on business rules, software functions and features and policies and procedures developed for Medical Device Distributor claims access to PharmaNet. Neither the Manager nor any Authorized Person may have access to PharmaNet until that person has completed training (with the exception of access that occurs during the training process, solely as necessary for the training).

6. Responsibilities of the Manager

At such time as the PharmaNet connection is available to the Distributor Site, the Manager must:

- equip the Distributor Site with a computer system which meets the requirements set out in the current HealthNet/BC Professional and Software Compliance Standards;
- install any terminal capable of accessing and displaying any PharmaNet information in an area of the Distributor Site which (i) is only accessible to the Manager and Authorized Persons, and (ii) is under the supervision of the Manager;
- arrange to connect the system to PharmaNet;
- upgrade computer software as needed to comply with changes to the HealthNet/BC Professional and Software Compliance Standards;
- Supervise access to PharmaNet by any Authorized Person; and
- reverse information in the PharmaNet database, pertaining to devices not released to the patient or the patient’s representative and record the reason for the reversal within thirty days of the original entry of the information on PharmaNet.
7. Individuals Authorized to Access PharmaNet

PharmaNet may only be accessed on behalf of the Medical Device Distributor (MDD) by the following:

a) the Manager;
b) an Authorized Person under the supervision of the Manager; or
c) Software Support Organizations (SSOs) - The Manager or delegate may authorize one or more persons employed by or contracted to a SSO temporary access to PharmaNet claims. These authorizations are only for the extent necessary and for the least amount of time required for the installation, testing, maintenance or repair of the hardware or software required for the MDD to connect to and to access PharmaNet claims.

Prior to allowing such access, the Manager must obtain from an authorized representative of the SSO a signed copy of the document “Medical Device Distributor – Software Vendor PharmaNet Third Party Confidentiality Undertaking (URL: https://www.health.gov.bc.ca/exforms/das/4552fil.pdf). This document must be signed by the SSO’s authorized representative, the technician employed by the SSO who will have access to PharmaNet at the Distributor Site and the Manager of the Distributor site.

Each signature must be witnessed. A person may witness more than one signature, but must sign for each signature they witness.

Each signed form must be retained on file at the Distributor Site.

The MDD must make available all confidentiality undertakings on request of the Ministry of Health Services.

Identify delegate of Manager who may authorize access to an SSO and indicate the individual’s functions:

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________
8. Security

The Manager and each Authorized Person will be assigned a user ID and password provided by a Software Support Organization (SSO). The Manager and Authorized Persons shall not:

- Permit any third-party to use any user IDs and passwords provided to access PharmaNet;
- Divulge, share or compromise any user IDs and passwords;
- Use, or attempt to use, the user ID or any password of any other person;
- Test or examine the security related to PharmaNet;
- Take any action that might reasonably be construed as altering, destroying or rendering ineffective the Patient Record information on PharmaNet;
- Alter the format or content of a print or display of any confidential information; or
- Use any wireless devices such as personal digital assistants, laptops or cellphones to access PharmaNet.

The use of wireless technology such as a wireless router or local area network is not permitted.

Any terminal and printers capable of displaying PharmaNet information must be located in a protected area and physically set in a manner that preserves patient confidentiality. Printing from PharmaNet is not permitted.

The Medical Device Distributor (MDD) must respect the patient’s right to confidentiality by endeavoring to ensure that MDD/patient dialogue with respect to devices and/or supplies takes place in an area where that discussion cannot be overheard by others.

The Ministry of Health Services (MOHS) may perform random unannounced spot audits and inspections relating to PharmaNet access at the Distributor Site, and the Manager must permit MOHS access to the Distributor Site and to all relevant MDD records for that purpose.
9. Patient Records

All Patient Records must be stored at the Distributor Site in a secure manner to protect patient confidentiality. All information relating to a patient shall be considered privileged and confidential and shall not be released to any person without the express consent of the patient.

No Medical Device Distributor (MDD) may, for commercial purposes, release or permit the release of, information or an abstract of information obtained from a patient, from a Patient Record, or from PharmaNet about a patient, which would permit the identity of the practitioner or the patient to be determined.

All Patient Records must be retained for a period of not less than three years. Notwithstanding this, a MDD must not destroy Patient Records until any audit or investigation is completed.

Disposal of Patient Records

A MDD must dispose of all records in a manner that preserves patient confidentiality:

a) paper records must be shredded or incinerated; and

b) computerized records must be rendered unreadable through the use of an appropriate mechanical, physical or electronic process and converted into such a form that they cannot be reconstructed in whole or in part.

A MDD must ensure that individual records are not lost or removed during the destruction process and that the resulting waste does not include fragments of readable personal information.

10. Patient Profiles

In cases where patients are physically present in the Distributor Site, the Manager or Authorized Person must positively identify patients prior to accessing PharmaNet.

- **New patients** should be asked for their British Columbia Care Card, or one primary or two secondary pieces of identification. (See Appendix E for a description of primary and secondary identification).
- **Returning patients** should be asked to confirm their Personal Health Number (PHN), name and address.
- Always verify the patient’s demographics when accessing PharmaNet by PHN. See Appendix E- Patient identification
- Any incorrect personal information related to the patient profile must be reported to the PharmaNet Help Desk.
  - Vancouver: 604-683-7151
  - Rest of B.C. 1-800-663-7100 (toll-free)
- No Medical Device Distributor may collect personal information regarding a patient unless the information relates directly to and is necessary for providing health care services to the patient or for related administrative purposes.
11. Claims Access Discrepancy Reporting

The Medical Device Distributor is required to complete routine claims access discrepancy reporting to identify apparent unauthorized accesses. As a minimum, this reporting will compare the accesses to PharmaNet with patient claims to ensure that access is by an Authorized Person within the prescribed window (access occurs during the business day the claim was entered onto PharmaNet). Additional access discrepancy reporting based on best practice privacy criteria is recommended.

**Identify the method used for creating access discrepancy reports:**

- [ ] Post-access reconciliation of the access log to patient visit
- [ ] Combination of near real-time notifications and post-access analysis of exceptions and patterns over multiple accesses

**Describe the manual and automated processes used for creating access discrepancy reports** *(note: Some Software Support Organizations may provide electronic reconciliation capabilities).*

**Describe any best practice criteria used for identifying potential inappropriate accesses.**

**Identify the frequency at which a designated person with the MDD will perform a review of an access discrepancy report.**

- [ ] Daily
- [ ] Weekly

A review of the access discrepancy report must be completed at least weekly by the designated person at the Distributor Site. A review of a selective access audit log report or access discrepancy report can be completed on demand.

The PharmaNet access log reports and access discrepancy reports will be retained for a minimum of three years and filed in ____________________________ (location).

12. PharmaNet Access Audits

All instances of apparent inappropriate access to PharmaNet or confidentiality breaches will be investigated by the Chief Executive Officer or other senior officer of the Medical Device Distributor (MDD), and will be escalated according to the MDD’s privacy breach procedures which must comply with the Office of the Information and Privacy Commissioner for British Columbia’s Key Steps in Responding to Privacy Breaches *(please see Appendix F)*

If the MDD knows that there has been an unauthorized disclosure of personal information in its custody or under its control, the MDD must immediately notify the Ministry of Health Services, Health Sector Information Management/Information Technology HelpDesk at (250) 952-1234.
13. Help Procedures

When there are problems accessing PharmaNet, the Medical Device Distributor’s (MDD) procedures for problem determination, escalation and resolution should be followed.

- For PharmaNet access software problems call ___________________ at __________ (Phone)
- For hardware problems call ____________________________ at __________ (Phone)
- For Internet problems call _______________________________ at __________ (Phone)
- For all other problems, call the PharmaNet Help Desk at the number listed below. The MDD should contact its Software Support Organization for all system-related problems before contacting the PharmaNet Help Desk.
  - Vancouver: 604-683-7151
  - Rest of B.C. 1-800-663-7100 (toll-free)

14. Downtime

The PharmaNet system has a scheduled downtime from 12:00 am (Midnight) until 08:00 a.m. every Thursday morning. Generally the system is down for less than 4 hours rather than the full 8-hour period.

15. Patient Keyword

A patient may have assigned a keyword to restrict access to the patient’s PharmaNet record. The patient must supply the keyword for access to occur. If the patient supplies a keyword, it must be removed from all Medical Device Distributor records relating to the patient. It is permissible to store a Patient Keyword on the local system if the patient gives consent.

16. Miscellaneous

The Manager and Authorized Persons are responsible for reviewing fan-out messages (PharmaNet Participant Messaging) routinely.

PharmaNet Participant Messaging can be delivered using the most expedient method possible to alert users. This delivery method could include an electronic bulletin, electronic alerting system or the messages can be printed and manually distributed.

Identify the method used to notify Medical Device Distributor Claims Access to PharmaNet users of PharmaNet Participant Messaging:

_______________________________________________________________________

_______________________________________________________________________

Identify the location where these messages will be filed: ________________________ (location)
Appendix A – Acknowledgement of Completion of Confidentiality Procedures for Medical Device Distributor Claims Access to PharmaNet

Medical Device Distributor Claims Access to PharmaNet
ACKNOWLEDGEMENT OF COMPLETION OF CONFIDENTIALITY PROCEDURES

("the Distributor"): ____________________________
name of Medical Device Distributor

("Distributor Site"): ____________________________
site street address and name (if different than Distributor name) of Medical Device Distributor site

I, ____________________________, Chief Executive Officer or other senior officer of the Distributor
name of CEO or other senior officer of the Distributor

and I, ____________________________, ____________________________,
name of person having supervisory responsibility at the Distributor site title of person having supervisory responsibility

have implemented procedures to ensure confidentiality and privacy of patient records.

We acknowledge that we have:

• obtained signed PharmaNet Confidentiality Undertakings for all persons authorized to access PharmaNet information within the Distributor Site;

• become familiar with the terms and conditions of the Medical Device Distributor Claims Access to PharmaNet Policies and Procedures ("the Policies and Procedures") and the latest version of the Common Volumes and Volumes 2 and 3 (Pharmacy) of the PharmaNet Professional and Software Compliance Standards ("the Standards"), limited to the relevant set of claims transactions (as identified below);

• documented policy and procedures related to PharmaNet access which are in compliance with the terms and conditions of the Policies and Procedures and the Standards;

• provided adequate training regarding the confidentiality policies and procedures referred to above for all persons authorized to access PharmaNet at the Distributor Site;

• agreed to only use the following claims transactions for Distributor access to PharmaNet:
  1. Adjudicate claims – submission, reversal and re-transmission of a claim
  2. View own previous transactions
  3. View store totals
  4. Input a Personal Health Number and verify the claim will be submitted for the correct person

  • Note: Medical Device Distributors will not be able to perform the following tasks:
    1. Update personal information such as keywords, address, or profile information
    2. Create Personal Health Numbers
    3. View prescriber information
    4. Enter in a partial name and retrieve a list of similar names
    5. View First Data Bank drug monograph information
    6. Modify or view eligibility records (Software Vendors are not able to submit this transaction)
    7. Profile mailing request
- agreed to only allow remote access to personal information in PharmaNet by Software Support Organizations from within Canada and only for the purposes of supporting the software;
- prepared informational material to be available to members of the general public who request more information regarding Distributor access to PharmaNet;
- appointed Distributor employee(s) who are able to respond to questions regarding Distributor access to PharmaNet.

We further undertake to permit the members of the Ministry of Health Services, Health Sector INVIT Compliance Team to perform unannounced audits and inspections at the Distributor Site, or at any other premises where records relating to Distributor access to PharmaNet are maintained, in order to verify compliance with the terms of this document.

We acknowledge that failure to comply with the above procedures and requirements at any time may result in the immediate termination of Distributor access to PharmaNet, in the sole discretion of the Ministry of Health Services.

<table>
<thead>
<tr>
<th>SIGNED AND DELIVERED BY</th>
<th>IN THE PRESENCE OF</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNATURE OF CHIEF EXECUTIVE OFFICER</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
<tr>
<td>FIRST NAME OF CHIEF EXECUTIVE OFFICER</td>
<td>FIRST NAME OF WITNESS</td>
</tr>
<tr>
<td>BUSINESS MAILING ADDRESS OF CHIEF EXECUTIVE OFFICER</td>
<td>ADDRESS</td>
</tr>
<tr>
<td>EMAIL ADDRESS OF CHIEF EXECUTIVE OFFICER</td>
<td></td>
</tr>
<tr>
<td>SIGNATURE OF MANAGER</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
<tr>
<td>FIRST NAME OF MANAGER</td>
<td>FIRST NAME OF WITNESS</td>
</tr>
<tr>
<td>BUSINESS MAILING ADDRESS OF MANAGER</td>
<td>ADDRESS</td>
</tr>
<tr>
<td>EMAIL ADDRESS OF MANAGER</td>
<td></td>
</tr>
</tbody>
</table>

Please return original to:
Ministry of Health Services
Data Access, Research and Stewardship
1-2, 1515 Blanshard Street
Victoria, BC V8W 3C8

HelpDesk: (250) 952-1234
Fax: (250) 952-1119
Appendix B – Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Manager

BACKGROUND:
A. Her Majesty the Queen in Right of the Province of British Columbia, as represented by the Ministry of Health Services (“the Province”) has agreed to allow ___________________________ name of Medical Device Distributor

(“the Distributor”) claims access to the provincial computerized pharmacy network and database known as “PharmaNet” at ___________________________ address of Medical Device Distributor Site

(“the Distributor Site”).

B. I am the individual with supervisory responsibility (“the Manager”) in relation to (a) the operation of the Distributor Site, and (b) the employees of the Distributor working at the Distributor Site.

UNDERTAKING:

1. ___________________________ name of manager am the Manager of the Distributor Site.

I hereby acknowledge that I agree with the following statements and undertakings:

2. I have read, understood, and will comply with:
   (a) the Personal Information Protection Act, S.B.C. 2003, c. 63; and
   (b) the Medical Device Distributor Claims Access to PharmaNet Policies and Procedures (“Policies and Procedures”) and the latest version of the Common Volumes and Volumes 2 and 3 (Pharmacy) of the PharmaNet Professional and Software Compliance Standards (“the Standards”), limited to the relevant set of claims transactions (as identified in the Acknowledgement of Completion of Confidentiality Procedures for Medical Device Distributor Claims Access to PharmaNet).

3. I will access PharmaNet only if:
   (a) the access is required for the purposes of carrying out my employment or other duties at the Distributor Site;
   (b) the access is for the purpose of submitting a PharmaCare claim to the British Columbia PharmaCare Program, or for the purpose of receiving confirmation or denial of payment of a PharmaCare claim from the British Columbia PharmaCare Program; and
   (c) the purpose and manner of access is consistent with the Policies and Procedures.

4. I may authorize one or more persons (“Authorized Persons”) to access PharmaNet only if:
   (a) the Authorized Person is under my supervision;
   (b) the Authorized Person requires access to PharmaNet for the purposes of carrying out the person’s employment or other duties at the Distributor Site;
   (c) the access is for the purpose of submitting a PharmaCare claim to the British Columbia PharmaCare program, or for the purpose of receiving confirmation or denial of a PharmaCare claim from the British Columbia PharmaCare program;
   (d) the purpose and manner of the access to PharmaNet by the Authorized Person is consistent with the Policies and Procedures; and
   (e) the Authorized Person has signed an Undertaking of Confidentiality.
4. I will maintain all information accessed by me or disclosed to me from PharmaNet in confidence, unless I am required to disclose the information by law, or at the request of the patient to whom the information relates.

5. I will protect all information accessed by me or disclosed to me from PharmaNet by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of information, files or records containing information from PharmaNet.

6. I will not:
   (a) permit any person to use any user IDs or passwords provided to me to access PharmaNet;
   (b) divulge, share or compromise any user IDs or passwords;
   (c) use or attempt to use the user ID or password of any other person;
   (d) test or examine the security related to PharmaNet;
   (e) take any action that might reasonably be construed as altering, destroying, or rendering ineffective any information contained within PharmaNet;
   (f) print any information contained within PharmaNet; or
   (g) use any wireless technology such as a wireless router, local area network or personal digital assistant to access PharmaNet.

7. If an inspection reveals that I am in breach of the terms of this Undertaking, in addition to any legal remedy that the Province may have against me:
   (a) the Province may notify the Chief Executive Officer or other senior officer of the Distributor in respect of any suspected inappropriate access to PharmaNet by me or by any Authorized Person;
   (b) my authority to access PharmaNet may be terminated in the sole discretion of the Province; and
   (c) the authority of the Distributor to access PharmaNet from the Distributor Site may be terminated in the sole discretion of the Province.

<table>
<thead>
<tr>
<th>SIGNED AND DELIVERED BY</th>
<th>IN THE PRESENCE OF</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNATURE OF MANAGER</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>DATE SIGNED</td>
<td>WITNESS SIGNATURE</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PRINT NAME OF MANAGER</td>
<td>WITNESS SIGNATURE</td>
</tr>
<tr>
<td>PRINT NAME OF WITNESS</td>
<td>PHONE NUMBER</td>
</tr>
<tr>
<td>BUSINESS MAILING ADDRESS</td>
<td>ADDRESS</td>
</tr>
<tr>
<td>EMAIL ADDRESS OF MANAGER</td>
<td></td>
</tr>
</tbody>
</table>
Appendix C – Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Authorized Person

BACKGROUND:
A. Her Majesty the Queen in Right of the Province of British Columbia, as represented by the Ministry of Health Services ("the Province") has agreed to allow ________________________________ name of Medical Device Distributor
("the Distributor") claims access to the provincial computerized pharmacy network and database known as "PharmaNet" at ________________________________ address of Medical Device Distributor Site
("the Distributor Site").

B. ________________________________ name of individual with supervisory responsibilities at the Distributor Site ("the Manager")
has signed a "Medical Device Distributor Claims Access to PharmaNet Undertaking of Confidentiality by Manager" form.

C. Authorized persons are permitted to access PharmaNet from the Distributor Site for PharmaCare claims purposes.

UNDERTAKING:

I, ________________________________, am a ________________________________ working at the Distributor Site.

I hereby acknowledge that I agree with the following statements and undertakings:

1. I have read, understood, and will comply with:
   (a) the Personal Information Protection Act, S.B.C. 2003, c. 63; and
   (b) the Medical Device Distributor Claims Access to PharmaNet Policies and Procedures ("Policies and Procedures") and the latest version of the Common Volumes and Volumes 2 and 3 (Pharmacy) of the PharmaNet Professional and Software Compliance Standards ("the Standards"), limited to the relevant set of claims transactions (as identified in the Acknowledgement of Completion of Confidentiality Procedures for Medical Device Distributor Claims Access to PharmaNet).

2. I will access PharmaNet only if:
   (a) I am authorized to do so by the Manager;
   (b) the access is under the supervision of the Manager;
   (c) the access is required for the purposes of carrying out my employment or other duties at the Distributor Site;
   (d) the access is for the purpose of submitting a PharmaCare claim to the British Columbia PharmaCare Program, or for the purpose of receiving confirmation or denial of payment of a PharmaCare Claim from the British Columbia PharmaCare Program;
   (e) the purpose and manner of access is consistent with the Policies and Procedures.

3. I will maintain all information accessed by me or disclosed to me from PharmaNet in confidence, unless I am required to disclose the information by law, or at the request of the patient to whom the information relates.
4. I will protect all information accessed by me or disclosed to me from PharmaNet by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of information, files or records containing information from PharmaNet.

5. I will not:
   (a) permit any person to use any user IDs or passwords provided to me to access PharmaNet;
   (b) divulge, share or compromise any user IDs or passwords;
   (c) use or attempt to use the user ID or password of any other person;
   (d) test or examine the security related to PharmaNet;
   (e) take any action that might reasonably be construed as altering, destroying, or rendering ineffective any information contained within PharmaNet;
   (f) print any information contained within PharmaNet; or
   (g) use any wireless technology such as a wireless router, local area network or personal digital assistant to access PharmaNet.

6. If an inspection reveals that I am in breach of the terms of this Undertaking, in addition to any legal remedy that the Province may have against me:
   (a) the Province may notify the Manager in respect of any suspected inappropriate access to PharmaNet by me; and
   (b) my authority to access PharmaNet may be terminated in the sole discretion of the Province.
Appendix D – Medical Device Distributor – Software Vendor
PharmaNet Third Party Confidentiality Undertaking

<table>
<thead>
<tr>
<th>Between:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Device Distributor Site Manager (“the Manager”)</td>
<td>Medical Device Distributor Name</td>
</tr>
<tr>
<td>Medical Device Distributor Site Address (“the Distributor Site”)</td>
<td>MDU Contact Telephone No.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>And:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Vendor Technician Name (“the Technician”)</td>
<td>Software Vendor Company Name (“the Software Vendor”)</td>
</tr>
<tr>
<td>Software Vendor Company Address</td>
<td>Software Vendor Telephone No.</td>
</tr>
</tbody>
</table>

The Manager hereby authorizes the Technician identified above temporary custodial access to the computer database and its supporting programs in the Distributor Site for the purposes of PharmaNet program updates and maintenance.

The authorization is granted with the proviso that the Software Vendor employing the Technician and the Technician understand and promise to abide by the following terms and conditions:

1. The Software Vendor and the Technician will not access or use any clinical or patient information for any purpose other than as stated above.

2. The Software Vendor and the Technician will at all times treat as confidential information referred to in (1), and will not participate in or permit the unauthorized publication, release or disclosure of same, and will continue to do so following the expiration of any contracts currently existing between themselves and the Medical Device Distributor named in this document.

3. The Software Vendor and the Technician will at all times treat as confidential all information relating to the security and management of PharmaNet and the computer system within the PharmaCare Access Site, and will continue to do so following the expiration of any contracts currently existing between themselves and the Medical Device Distributor named in this document.

4. The Software Vendor and the Technician agree to adhere to all policies and procedures issued by the Medical Device Distributor or the Manager consistent with all legislation, policies, procedures or standards issued by the College of Pharmacists of British Columbia, the Province of British Columbia or its Ministry of Health Services, related to the confidentiality, privacy or security of information.

<table>
<thead>
<tr>
<th>SIGNED AND DELIVERED BY</th>
<th>IN THE PRESENCE OF</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNATURE OF AUTHORIZED REPRESENTATIVE OF SOFTWARE VENDOR</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
<tr>
<td>SIGNATURE OF TECHNICIAN</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
<tr>
<td>SIGNATURE OF MANAGER</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
<tr>
<td>SIGNATURE OF AUTHORIZED REPRESENTATIVE OF SOFTWARE VENDOR</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
<tr>
<td>SIGNATURE OF TECHNICIAN</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
<tr>
<td>SIGNATURE OF MANAGER</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
<tr>
<td>SIGNATURE OF AUTHORIZED REPRESENTATIVE OF SOFTWARE VENDOR</td>
<td>DATE SIGNED</td>
</tr>
<tr>
<td>PHONE NUMBER</td>
<td></td>
</tr>
</tbody>
</table>
Appendix E – Patient Identification

Prior to releasing information from PharmaNet to a patient, the Manager or Authorized Person must take all reasonable steps to positively identify the patient or the patient’s personal representatives, in compliance with PharmaNet standards as follows:

a) viewing one (1) piece of primary identification; or
b) viewing two (2) pieces of secondary identification.

Primary Documents which are acceptable to the Ministry of Health Services:

- Birth Certificate
- Canadian Citizenship ID Card
- Canadian Record of Landing or Confirmation of Permanent Residence or Permanent Resident Card
- Canadian Issued Student Authorization or Study Permit
- Canadian Issued Employment Authorization or Work Permit
- Canadian Issued Visitor Authorization or Temporary Resident Visa
- Diplomatic Passport
- Federal Minister’s Permit, approved by BC Minister of Health Temporary Resident Permit

Secondary Documents which are acceptable to the Ministry of Health Services:

A secondary identification document is a trusted document containing either a photograph or signature (or both) that identifies an individual as being who he or she claims to be and supports the personal information supplied by the individual.

- Driver’s License
- Passport
- Native Status Card (Issued by Indian and Northern Affairs Canada)
- Canadian Forces ID Card
- Canadian Police Identification Card
- Provincial or Territorial Identification Card
- Naturalization Certificate
- Consular Identity Card (External Affairs Identification Certificate or Card)
- Parole Certificate Identification Card
- Correctional Service Conditional Release Card

The BC Personal Health Number (PHN) is the provincial standard for identifying clients of the health care system and is needed to retrieve or update patient information. The existence of a PHN does not imply eligibility for health care services in BC, or provide any indication of an individual’s benefit status.
Appendix F – Privacy Breach Response Procedures

KEY STEPS IN RESPONDING TO PRIVACY BREACHES

June 2008

Purpose
The purpose of this document is to provide guidance to public bodies and organizations when a privacy breach occurs. Organizations and public bodies should take preventative steps prior to a breach occurring. See the OIPC personal information security guidelines for ideas on how to help prevent security breaches:
http://www.oipc.bc.ca/pdfs/private/PhysicianSecurityofpersonalinformation.pdf.

What is a privacy breach?
A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is “unauthorized” if it occurs in contravention of Personal Information Protection Act or part 3 of the Freedom of Information and Protection of Privacy Act. The most common privacy breach happens when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong person.

Privacy Breach Checklist
The OIPC has created a privacy breach checklist that allows public bodies and organizations to complete an analysis of the privacy breach using the four key steps described below. The privacy breach checklist is available at:
http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Checklist(June2008).pdf.

Four key steps in responding to a privacy breach
The most important step you can take is to respond immediately to the breach. You should undertake steps 1, 2 and 3 below immediately following the breach.

1 These key steps can assist both public bodies that are subject to the Freedom of Information and Protection of Privacy Act and organizations that are subject to the Personal Information Protection Act.
and do so simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies.

**Step 1: Contain the Breach**

You should take immediate common sense steps to limit the breach. These steps would include:

- Immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, revoking or changing computer access codes or correcting weaknesses in physical security.

- Activate your breach management policy. If you do not have a breach management policy take the following steps:
  
  o Designate an appropriate individual to lead the initial investigation. This individual should have the authority within the public body or organization to conduct the initial investigation and make initial recommendations. If necessary a more detailed investigation may subsequently be required.

  o Immediately contact your Director/Manager of Information and Privacy (DMIP) or your privacy officer and/or the person responsible for security in your organization. Determine others who need to be made aware of the incident internally at this preliminary stage.

  o Determine whether a breach response team must be assembled which could include representatives from appropriate business areas and should include the Director/Manager of Information and Privacy (DMIP) or your privacy officer and/or person responsible for security.

  o Notify the police if the breach involves theft or other criminal activity.

- Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or that will allow you to take appropriate corrective action.

---

2 The OIPC has created a template breach management policy that public bodies and organizations may use to develop their own breach management policy at: [http://www.opc.bc.ca/pdfs/Policy/Privacy_Breach_Management_Policy_Template(June2008).pdf](http://www.opc.bc.ca/pdfs/Policy/Privacy_Breach_Management_Policy_Template(June2008).pdf)
Step 2: Evaluate the Risks Associated with the Breach

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following factors in assessing the risks:

(i) **Personal Information Involved**
- What data elements have been breached? Generally, the more sensitive the data, the higher the risk. Some personal information is more sensitive than others (e.g., health information, government-issued pieces of identification such as social insurance numbers, driver's licence and health care numbers and financial account numbers such as credit or debit card numbers that could be used for identity theft.)
- A combination of personal information is typically more sensitive than a single piece of personal information.
- What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?
- What is the context of the personal information involved? For example, name and address in a phone book would be less sensitive than name and address on a list of clients receiving counselling or a list of clients away on holiday.

(ii) **Cause and Extent of the Breach**
- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- Was the information lost or stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Is the information encrypted or otherwise not readily accessible?
- Has the information been recovered?
- What steps have you already taken to minimize the harm?
- Is this a systemic problem or an isolated incident?

(iii) **Individuals Affected by the Breach**
- How many individuals are affected by the breach?
- Who was affected by the breach: employees, public, contractors, clients, service providers, other organizations?
(iv) **Foreseeable Harm From the Breach**

- Who is in receipt of the information? For example, a stranger who accidentally receives personal information and voluntarily reports the mistake is less likely to misuse the information than an individual suspected of criminal activity.
- Is there any relationship between the unauthorized recipients and the data subject? A close relationship between the victim and the recipient may increase the likelihood of harm—an estranged spouse is more likely to misuse information than a neighbour.
- What harm to the individuals will result from the breach? Harm that may occur includes:
  - security risk (e.g., physical safety)
  - identity theft or fraud
  - loss of business or employment opportunities
  - hurt, humiliation, damage to reputation or relationships
- What harm could result to the public body or organization as a result of the breach? For example:
  - loss of trust in the public body or organization
  - loss of assets
  - financial exposure
  - loss of contracts/business
- What harm could result to the public as a result of the breach? For example:
  - risk to public health
  - risk to public safety.

**Step 3: Notification**

Notification of affected individuals can be an important mitigation strategy in the right circumstances. The key consideration overall in deciding whether to notify should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed. Review your risk assessment to determine whether or not notification is appropriate. The OIPC has created a breach notification assessment tool to assist public bodies and organizations in determining when and how to notify individuals. The tool is available at: [http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf](http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf).

(i) **Notifying Affected Individuals**

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:
Legislation requires notification;
Contractual obligations require notification;
There is a risk of identity theft or fraud (usually because of the type of information lost/stolen/accessed/disclosed, such as SIN, banking information, identification numbers);
There is a risk of physical harm (if the loss puts an individual at risk of stalking or harassment);
There is a risk of hurt, humiliation or damage to reputation (for example when the information lost includes medical or disciplinary records);
There is a risk of loss of business or employment opportunities (if the loss of information could result in damage to the reputation of an individual, affecting business or employment opportunities);
There is a risk of loss of confidence in the public body or organization and/or good customer/client relations dictates that notification is appropriate.

(ii) When and How to Notify

When: Notification of individuals affected by the breach should occur as soon as possible following the breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method of notification is direct – by phone, letter or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

(iii) What Should be Included in the Notification?

Notifications should include the following pieces of information:

Date of the breach;
Description of the breach;
Description of the information inappropriately accessed, collected, used or disclosed;
Risk(s) to the individual caused by the breach;
The steps taken so far to control or reduce the harm;
Future steps planned to prevent further privacy breaches;
Steps the individual can take to further mitigate the risk of harm (e.g. how to contract credit reporting agencies to set up a credit watch,
information explaining how to change a personal health number or driver's licence number);  
- Contact information of an individual within the public body or organization who can answer questions or provide further information;  
- Privacy Commissioner contact information and the fact that individuals have a right to complain to the Office of the Information and Privacy Commissioner. If the public body or organization has already contacted the Privacy Commissioner, include this detail in the notification letter.

(iv) Other Sources of Information

As noted above, the breach notification letter should include a contact number within the public body or organization in case affected individuals have further questions. In anticipation of further calls, you should prepare a list of frequently asked questions and answers to assist staff responsible for responding to the further inquiries.

(v) Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

- Police: if theft or other crime is suspected
- Insurers or others: if required by contractual obligations
- Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies
- Other internal or external parties not already notified: Your investigation and risk analysis may have identified other parties impacted by the breach such as third party contractors, internal business units or unions.
- Office of the Information and Privacy Commissioner: The following factors are relevant in deciding when to report a breach to the OIPC:
  - the sensitivity of the personal information;
  - whether the disclosed information could be used to commit identity theft;
  - whether there is a reasonable chance of harm from the disclosure including non pecuniary losses;
  - the number of people affected by the breach;
  - whether the information was fully recovered without further disclosure;
Privacy Breaches – Key Steps – Office of the Information & Privacy Commissioner

- your organization or public body requires assistance in developing a procedure for responding to the privacy breach, including notification and/or,
- to ensure steps taken comply with the organization’s or public body’s obligations under privacy legislation.

To notify the Office of the Information and Privacy Commission, complete the Privacy Breach Checklist located at:
http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Checklist(June2008).pdf

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long term safeguards against further breaches. Policies should be reviewed and updated to reflect the lessons learned from the investigation and regularly after that. Your resulting plan should also include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented. Staff of organizations should be trained to know the organization’s privacy obligations under the Personal Information Protection Act. Staff of public bodies should be trained to know the public body’s privacy obligations under the Freedom of Information and Protection of Privacy Act. For further ideas on how to prevent privacy breaches, see the personal information security guidelines at:
http://www.oipc.bc.ca/pdfs/private/PhysicianSecurityofpersonalinformation.pdf

This document is for general information only. It is not intended to be, and cannot be relied upon as, legal advice or other advice. Its contents do not fetter, bind or constitute a decision or finding by, the Office of the Information and Privacy Commissioner (OIPC) with respect to any matter, including any complaint, investigation or other matter, respecting which the OIPC will keep an open mind. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization and public body.