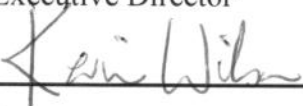
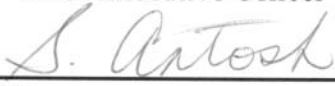


<b>Subject/Title:</b>  <i>PHARMACEUTICAL INFORMATION PROGRAM (PIP) JOINT SERVICE &amp; ACCESS POLICY</i>	<b>Reference Number:</b> <b>001</b>
<b>Approving Authorities:</b>  <b>Drug Plan and Extended Benefits Branch, Ministry of Health, Saskatchewan (the "Ministry")</b>  <b>Name:</b> Kevin Wilson, Drug Plan and Extended Benefits Branch <b>Title:</b> Executive Director   _____ Signature	<b>Effective Date:</b> <b>June 24, 2009</b>
<b>eHealth Saskatchewan ("eHealth")</b>  <b>Name:</b> Susan Antosh  <b>Title:</b> Chief Executive Officer   _____ Signature	<b>Revision Dates:</b> <b>March 10, 2016</b>

## 1. *High Level Policy*

The information stored in the Pharmaceutical Information Program ("PIP") constitutes personal health information and is subject to the provisions of *The Health Information Protection Act* (Sask) ("HIPA") and other provincial legislation as mentioned below, and in some cases the *Personal Information Protection and Electronic Documents Act* (Canada) ("PIPEDA").

Your use of the personal health information within PIP is restricted to authorized health purposes only as described in this Policy. Use or disclosure for any other purpose is strictly prohibited. Viewing patient profiles in PIP is classified as a use.

## 2. *Background/Scope/Purpose*

---

Pursuant to section 3.3 of *The Prescription Drugs Act* (Sask), the Ministry is authorized to establish a database (“PIP”) of personal health information with respect to all drugs prescribed or dispensed to persons in Saskatchewan.

The Ministry controls the personal health information stored within PIP and therefore pursuant to section 2(t) of HIPA, the Ministry is the trustee of this information.

The Ministry collects and uses the personal health information stored in PIP for the purposes of providing or supporting a healthcare service for the subject individual, facilitating payment for healthcare services (i.e. processing drug plan claims) and/or the purposes outlined in *The Prescription Drugs Act* (Sask).

The Ministry discloses personal health information to other trustees (and in limited circumstances, to non-trustees who are healthcare providers in Alberta and Manitoba providing health services to Saskatchewan residents in Border Communities) through the view and print functions within PIP for these same purposes.

In the initial rollout of PIP, each organization (the “User Organization”) collecting and using the personal health information stored in PIP was required to execute a Data Access Agreement before being given User-IDs for PIP.

This Service & Access Policy (“Policy”) amends and replaces the existing Data Access Agreements governing the rights and responsibilities of existing User Organizations in the use of PIP. This Policy becomes effective for the existing User Organizations as follows:

- for each existing User Organization which is not a Regional Health Authority (“RHA”) upon 30 days notice in accordance with subsection 8(a) of the PIP Application Data Access Agreement; and
- for each RHA upon receipt by the Ministry of written acceptance from the RHA.

The purpose of this Policy is to:

- (a) set out the responsibilities and rules of collection, use, and disclosure for User Organizations and its Users who are collecting, using and disclosing PIP Data; and
- (b) act as an information management services agreement between each User Organization and eHealth.

This Policy applies to all existing User Organizations as discussed above, in addition to:

- (a) all new User Organizations that collect, use or disclose PIP Data within PIP; and
- (b) all healthcare providers approved by the User Organizations who collect, use or disclose the PIP Data on behalf of the User Organization within PIP.

By signing on or connecting to the PIP application, a User Organization's Users are viewing confidential personal health information. As a condition to allowing the User Organization's Users to sign on or connect to the PIP application, each User Organization agrees to abide by and be legally bound by this Policy.

### **3. *Legislative Authority/Resources***

---

*The Health Information Protection Act, Saskatchewan ("HIPA") and The Health Information Protection Regulations*

*Personal Information Protection and Electronic Documents Act, Federal ("PIPEDA")*

*The Prescription Drugs Act, Saskatchewan and Prescription Drugs Regulations, 1993*

Please see the reference materials at the Ministry of Health website

<http://www.saskatchewan.ca/residents/health/accessing-health-care-services/your-personal-health-information-and-privacy> and the Saskatchewan Office of the Information and Privacy Commissioner website at [www.oipc.sk.ca](http://www.oipc.sk.ca) for further information regarding HIPA.

### **4. *Interpretation***

---

Please see Schedule "A" to this Policy for a Glossary of Terms.

### **5. *Detailed Policy***

---

#### **5.1 Accountability.**

##### **5.1.1 User Organization Responsibilities**

Each User Organization shall:

- (a) appoint a User Organization Representative who will be responsible for privacy for PIP, and a User Organization Approver (who may be the same individual as the User Organization Representative) who will be responsible to manage and designate Users and User roles for the User Organization;
- (b) provide eHealth and the Ministry with the contact information for its User Organization Representative and (where applicable) its User Organization Approver;
- (c) with respect to PIP Data within its custody or control or within systems within its custody or control, establish written policies and procedures to maintain administrative, technical and physical safeguards that will:

- (i) protect the integrity, accuracy and confidentiality of the information;
- (ii) protect against any reasonably anticipated:
  - 1. threat or hazard to the security or integrity of the information;
  - 2. loss of the information; or
  - 3. unauthorized viewing, use, disclosure, modification or deletion of the information; and
- (iii) otherwise ensure compliance with HIPA by its employees;
- (d) comply with all applicable laws including without limitation HIPA and, where applicable, PIPEDA. It is important to note that the Saskatchewan Office of the Information and Privacy Commissioner has stated as follows:

(A) trustee cannot rely on the provisions in HIPA for collection, use and disclosure of personal health information without express or implied consent in sections 26, 27 and 28 unless that trustee has first satisfied the general duties in sections 9, 10, 16, 19, 23.<sup>1</sup>

It is the responsibility of each User Organization to ensure it has authority and consent to collect, use, disclose and enter PIP Data as outlined in this Policy.

### **5.1.2 Collection, Use and Disclosure of PIP Data**

The Ministry is the trustee of PIP Data while it is stored or transmitted within the Ministry's systems.

Once the PIP Data has been incorporated into the User Organization's records this Policy will no longer apply. In such event:

- (a) Section 20 of HIPA will apply to all User Organizations who are trustees under HIPA. Section 20 states as follows:

**20(1)** Where one trustee discloses personal health information to another trustee, the information may become a part of the records of the trustee to whom it is disclosed, while remaining part of the records of the trustee that makes the disclosure.

**(2)** Where personal health information disclosed by one trustee becomes a part of the records of the trustee to whom the information is disclosed, the trustee to whom the

---

<sup>1</sup> Saskatchewan Office of the Information and Privacy Commissioner Investigation Report H-2005-002, Prevention Program for Cervical Cancer at p. 80

(2) Where personal health information disclosed by one trustee becomes a part of the records of the trustee to whom the information is disclosed, the trustee to whom the information is disclosed is subject to the same duties with respect to that information as the trustee that discloses the information.

For example if the User prints off the PIP Data for a patient and places it within the User Organization's medical record for the patient, the User Organization will be subject to the same duties with respect to that information as the Ministry.

(b) Section 21 of HIPA will apply to User Organizations that are not included as trustees under HIPA. Section 21 states as follows:

**21** Where a trustee discloses personal health information to a person who is not a trustee, the trustee must:

(a) take reasonable steps to verify the identity of the person to whom the information is disclosed; and

(b) where the disclosure is made without the consent of the subject individual, take reasonable steps to ensure that the person to whom the information is disclosed is aware that the information must not be used or disclosed for any purpose other than the purpose for which it was disclosed unless otherwise authorized pursuant to this Act.

If the User Organization is a non-trustee, it specifically acknowledges that the PIP Data must not be used or disclosed for any purpose other than for an authorized health purpose as described in section 2 of this Policy and the User Organization has the consent of the subject individual. All non-trustee User Organizations must be specifically approved in writing by the Ministry.

If HIPA does not apply to a User Organization, that User Organization will be required to protect the confidentiality and security of the PIP Data to the same standard as outlined in this Policy and laws applicable within their jurisdiction (ex. the *Health Information Act* (Alberta)).

Each User Organization will be responsible for designating who within its organization will be entitled to collect, use and disclose the PIP Data within PIP. Each User Organization accepts responsibility for ensuring that authorized Users comply with this Policy and do not improperly use or disclose the PIP Data.

### **5.1.3 Entry of PIP Data**

Each User Organization will be responsible to determine who within its organization will be permitted to make use of the functionality which enables the entry of PIP Data into PIP, and to verify that each User with such permission is properly authorized for a particular role and has all necessary licenses and authorities associated with that role.

Each User Organization accepts responsibility for ensuring that the Users it authorized comply with this Policy and do not improperly enter PIP Data.

Each User Organization will be responsible to ensure that any PIP Data collected and provided by the User Organization and its Users is reasonably accurate, and that the User Organization has taken reasonable steps to ensure the accuracy of such PIP Data.

PIP Additional Data and PIP Prescription Data shall only be entered into PIP on an implied consent basis as described in the User training material.

### **5.1.4 Information Management Service Provider**

eHealth Saskatchewan (“eHealth”, formerly the Saskatchewan Health Information Network) will be acting as the information management service provider for PIP. eHealth will provide the following services in accordance with the Ministry’s instructions (“eHealth Services”):

- (a) establishing and maintaining the technical infrastructure for PIP within the eHealth Data Centre;
- (b) managing the networks within eHealth’s control required for PIP;
- (c) testing the above infrastructure and networks, along with their interfaces to other networks;
- (d) providing project management services for the development of PIP;
- (e) providing operation and technical support for PIP including help desk services;
- (f) providing database management and support services; and
- (g) de-identification and reporting services.

The eHealth Services may be further defined in a concept of operations or other detailed document prepared by eHealth, agreed to by the Ministry and provided to the User Organizations. eHealth may only use PIP Data on a need-to-know basis in order to provide the eHealth Services.

PIP will be centrally hosted on servers located within the eHealth Data Centre in Regina, Saskatchewan. Schedule “B” to this Policy describes the terms and conditions that apply

between the User Organizations and eHealth as the information management service provider for PIP.

#### **5.1.5 Border Community User Organizations**

Each Border Community User Organization shall comply with and be bound by Schedule “C” to this Policy as may be amended from time to time in accordance with this Policy.

#### **5.2 Identifying Purposes.**

PIP Data stored within the PIP Database shall only be collected, used and disclosed for the purpose of providing or supporting health care services for the subject individual, to facilitate payment for health services for the subject individual and/or purposes outlined in *The Prescription Drugs Act* (Sask). PIP Prescription Data and PIP Additional Data shall only be entered into PIP for the purpose of providing or supporting health care services to the subject individual or to facilitate payment for health services of the subject individual.

With the written consent of the Ministry, de-identified data (as defined in Schedule “A” to this Policy) from PIP may be used for monitoring, evaluation and research.

Collection, use and disclosure of the PIP Data stored within PIP for any other purpose, or entry of PIP Prescription Data or PIP Additional Data into PIP for any other purpose, must be pre-approved in writing by the Ministry.

#### **5.3 Consent.**

All User Organizations will:

- (a) carry out all patient communication policies and procedures related to PIP that may be approved by the Ministry from time to time;
- (b) refer all patients who wish to make use of PIP’s patient control option to the eHealth Privacy Service; and
- (c) ensure that PIP Data which is masked under PIP’s patient control option is used by Users only in accordance with the Ministry’s unmasking criteria.

#### **5.4 Limiting Collection, Use and Disclosure.**

The User Organizations and its authorized Users may only collect and use PIP Data stored within PIP on a need-to-know basis for an approved health purpose as per section 5.2. The need-to-know must be supported by the User’s relationship to the patient and specific health services being provided. The User Organization shall respect the User Roles defined within the application. Where PIP Data is disclosed to the User Organization through a system to system interface, the User Organization agrees to have appropriate User Roles defined in writing within the local system.



**5.5 Accuracy.**

All User Organizations and authorized Users will take reasonable steps to ensure the accuracy of any information entered into or updated by them within PIP and agree to follow any instructions or procedures approved by the Ministry from time to time.

**5.6 Testing.**

Whenever practical, de-identified data will be used by eHealth for testing PIP and its interfaces with other systems. Where identifiable PIP Data is required for such testing, it will only be used in accordance with testing plans submitted by eHealth and written approval is received from the Ministry.

**5.7 Safeguards.**

Each User Organization agrees that appropriate physical, organizational and technological measures as outlined in section 5.1.1(c) will be put in place within its organization to protect the security and confidentiality of the PIP Data and to ensure that this data is only used on a need-to-know basis for authorized health purposes as per section 5.2.

Each User Organization agrees to follow any security procedures approved by the Ministry from time to time.

**5.8 Openness.**

Each User Organization will ensure that its written privacy and security policies and procedures are available to the public.

**5.9 Individual Access/Amendment.**

Each User Organization agrees to address requests for a patient's access to one's own PIP Data within PIP and to take steps to verify the patient's identity before providing a patient with access to the PIP Data. Patients may also address requests for access to PIP Data within PIP directly to the Drug Plan and Extended Benefits Branch with the Ministry to be handled in accordance with its policies and procedures.

All patients making requests for amendments to PIP Data will be referred to the Ministry. Where necessary and appropriate the Ministry will consult with the User Organization that is the source of the data being amended. If an amendment cannot be made, a notation of the request will be included in the patient file.

With the consent of the patient, the User Organization which entered the PIP Prescription Data or PIP Additional Data may make an amendment requested by the subject individual. The Ministry, as trustee, retains the authority to determine what type of amendment should be made if a patient's request is not addressed to the satisfaction of the patient by the User Organization.



All User Organizations agree to have appropriate written policies, procedures and forms in place to facilitate access by a patient to PIP Data stored in PIP. The User Organizations recognize the importance of providing patients timely access to PIP Data stored in PIP. Written requests received pursuant to HIPA must be answered within 30 calendar days.

#### **5.10 Complaints.**

All complaints and breaches relating to PIP will be referred by the organization receiving the complaint, or having knowledge of the breach to the Ministry for investigation, review and resolution. The Ministry will involve other User Organizations where appropriate.

All User Organizations agree to have appropriate and reasonable written policies, procedures and forms to address privacy concerns, complaints or incidents, whether raised by patients or otherwise.

Any complaints may be forwarded by the patient to the Office of the Information and Privacy Commissioner (Sask). Please see the Privacy Breach Guidelines at [www.oipc.sk.ca](http://www.oipc.sk.ca) for assistance in dealing with specific complaints.

#### **5.11 Audits.**

Collection and use of PIP Data from PIP will be tracked and logged. Patient level reports showing what Users (or systems) have viewed (received) the PIP Data for a particular patient are available to that patient. All requests to receive this report should be forwarded to the eHealth Privacy Service.

#### **5.12 Overriding Provision.**

Nothing in this Policy is intended to be inconsistent with or contrary to any applicable laws or the rights and duties of User Organizations under applicable laws.

#### **5.13 Amendment of Policy.**

The Ministry may amend this Policy provided that any changes to Schedule “B” will require the written agreement of eHealth. Each amendment will become binding on a User Organization 30 days after notice of the amendment is provided to the User Organization.

### **6. *Procedures/Policies***

---

#### **6.1 Implementation.**

This Policy will be implemented as follows:

- (a) Each User Organization will receive a copy of this Policy and agree to be legally bound to this Policy in its application form to become a User Organization. Where the User Organization is already registered, it will confirm acceptance through other means such as written confirmation or electronic acceptance.
- (b) Each User will receive a copy of this Policy and agree to be legally bound to this Policy in the initial application form to obtain a User ID and password. Where the User is already registered, acceptance will be confirmed through other means such as electronic acceptance upon signing on to the system.
- (c) During training, each User will receive a copy of this Policy and a high level overview of the provisions explained to them.
- (d) When logging onto the application, Users will be reminded of the confidential nature of the information and that their user rights are subject to their compliance with this Policy.

Where the above implementation process is impractical for a particular User Organization, the User Organization will be required to follow an alternative process approved by the Ministry.

## **6.2 Additional Policies & Procedures.**

In addition to the obligations outlined in this Policy, all Users and User Organizations will be and remain bound to:

- (a) comply with all applicable laws, ethical requirements and guidelines;
- (b) comply with all additional policies, procedures and manuals related to PIP approved by the Ministry; and
- (c) comply with all other applicable policies and procedures related to their collection, use and disclosure of personal health information which may apply to their use of PIP. For example, Users employed or associated with an RHA will remain bound to comply with the policies and procedures of the RHA that protect the security and confidentiality of personal health information.

## **7. Term/Termination**

---

### **7.1 Term of Policy.**

This Policy shall come into force on the date on which it is approved by the Ministry, and shall remain in force until terminated in accordance with this Article. For greater certainty, the terms of this Policy will continue to apply to:

- (a) User Organizations;
- (b) Users; and
- (c) eHealth,

notwithstanding that any such party has withdrawn or been suspended or terminated in accordance with this Policy.

7.2 **Withdrawal by User Organization.**

A User Organization may withdraw from further involvement with PIP by providing 90 days notice in writing to eHealth and the Ministry.

7.3 **Suspension or Termination by Ministry.**

If the Ministry believes that a User or User Organization has not complied with the privacy laws applicable to it or with the terms of this Policy, the Ministry may suspend the User/User Organization's right to collect or use information within PIP under this Policy in whole or in part.

The Ministry shall inform the applicable User/User Organization of any suspension, and shall provide the User/User Organization an opportunity to make representations to the Ministry. The Ministry may then reinstate the User/User Organization's rights under this Policy or, if it appears to the Ministry that the User/User Organization will not or cannot comply with its obligations, the Ministry may terminate the User/User Organization's permission to collect or use PIP Data from PIP.

7.4 **Withdrawal by eHealth.**

eHealth may withdraw from participation in PIP by providing 90 days notice in writing to the Ministry. On receiving such notice the Ministry shall work with eHealth to facilitate the orderly transfer of the applicable eHealth Services to another provider.

**SCHEDULE A  
 GLOSSARY OF TERMS**

<p><b>“Border Community User Organization”</b></p>	<p>means a User Organization located in a community located in Alberta or Manitoba:</p> <ul style="list-style-type: none"> <li>- which is in reasonable proximity to the border with Saskatchewan;</li> <li>- whose community services are accessed by a significant number of Saskatchewan residents; and</li> <li>- which, as a result of the above two factors, has reached an agreement with the Drug Plan respecting the provision of services to Saskatchewan residents, or otherwise satisfied the Ministry that authorization to use PIP is required in order to provide service to patients resident in Saskatchewan;</li> </ul>
<p><b>“eHealth Privacy Service”</b></p>	<p>means the service operated to assist in addressing privacy and security issues and concerns raised by patients and to assist patients to obtain access to, amendment of, or masking of, their medication profile stored in PIP;</p>
<p><b>“de-identified data”</b></p>	<p>means PIP Data (including aggregated or transformed data) from which any information that may reasonably be expected to identify an individual has been removed;</p>
<p><b>“Drug Plan”</b></p>	<p>means the Drug Plan and Extended Benefits Branch, a branch within the Ministry;</p>
<p><b>“ECPI”</b></p>	<p>means the Drug Plan’s Enhanced Collection of Prescription Information program also commonly known as ADAPT – All Drugs All People Today;</p>
<p><b>“eHealth”</b></p>	<p>means eHealth Saskatchewan (formerly the Saskatchewan Health Information Network), the Treasury Board Crown Corporation which holds the licenses and contracts associated with the administration and management of PIP;</p>
<p><b>“healthcare provider”</b></p>	<p>means a health professional or an authorized employee who is employed by or associated with a User Organization. The term “associated with” means the healthcare provider is not employed but is providing contract services;</p>
<p><b>“HIPA”</b></p>	<p>means <i>The Health Information Protection Act</i> (Saskatchewan);</p>
<p><b>“the Ministry”</b></p>	<p>means the Saskatchewan Ministry of Health;</p>
<p><b>“medication profile”</b></p>	<p>means the profile of medication relating to a particular patient, consisting of a multiple pharmacy/clinic view of the patient’s prescription drugs profile reflecting the information which has been collected under the ECPI Program and any PIP Prescription Data and</p>

	PIP Additional Data;
<b>“patient”</b>	means an individual who is or will be obtaining a health service from a User Organization;
<b>“personal health information”</b>	means, with respect to a patient, whether living or deceased: (i) information with respect to the physical or mental health of the patient; (ii) information with respect to any health service provided to the patient; (iii) information with respect to the donation by the patient of any body part or any bodily substance of the patient or information derived from the testing or examination of a body part or bodily substance of the patient; (iv) information that is collected: (A) in the course of providing health services to the patient; or (B) incidentally to the provision of health services to the patient; or (v) registration information;
<b>“PIP”</b>	means the Pharmaceutical Information Program;
<b>“PIP Additional Data”</b>	means any of the following: - data with respect to a patient’s allergies and intolerances; - prescription notes; - responses to alerts within PIP; and - data with respect to drugs that are not included in ECPI;
<b>“PIP Data”</b>	means the data elements associated with PIP as described in Schedule “D” of the Phase 2.2 DPIA, as well as PIP Additional Data and PIP Prescription Data;
<b>“PIP Prescription Data”</b>	means prescription information related to prescriptions entered in PIP by a Prescriber but not yet dispensed;
<b>“PIPEDA”</b>	means the federal <i>Personal Information Protection and Electronic Documents Act</i> ;
<b>“Prescriber”</b>	means a healthcare provider who is authorized to prescribe prescription drugs and is confirmed as such by the User Organization Approver;
<b>“RHAs”</b>	means the Regional Health Authorities established pursuant to <i>The Regional Health Services Act</i> (Sask);
<b>“trustee”</b>	means a trustee as defined in HIPA;
<b>“User”</b>	means an individual who is employed by or associated with the Ministry or a User Organization who has been authorized to user

	rights into PIP;
<b>“User Organization”</b>	means a clinic, pharmacy, RHA or other organization outside the Ministry with user rights into PIP;
<b>“User Organization Approver”</b>	means the person who is authorized to designate Users and User roles for a User Organization; and
<b>“User Organization Representative”</b>	means the person who is designated as responsible for PIP privacy matters within a User Organization. This representative must have specific authority granted by the User Organization as described in section 58 of HIPA.

**SCHEDULE B**  
**EHEALTH SERVICE TERMS AND CONDITIONS**

BY ACCESS TO PIP USER ORGANIZATIONS ARE AGREEING TO THE TERMS AND CONDITIONS OUTLINED IN THIS SCHEDULE B.

1. Purpose

The purpose of this Schedule B to the PIP Joint Service & Access Policy (the “Policy”) is to describe the terms and conditions associated with the provision of the eHealth Services by eHealth to the User Organization.

Please see the Glossary attached as Schedule “A” to the Policy for defined terms.

2. Restrictions on Use and Disclosure of the PIP Object Code

Each User Organization agrees:

- (a) that, to the extent third party code is accessed or used, the User Organization will take all reasonable steps to protect and maintain the confidentiality of that code, at all times using the same care and discretion to avoid disclosure or dissemination of third party code as the User Organization uses with its own confidential information;
- (b) to take all reasonable steps to prohibit, and to cooperate with the Ministry in the prohibition of, the reverse engineering, decompilation or disassembly of third party code, or the making of derivative works of such code; and
- (c) to limit access to third party code to those users who have a need to know, unless written consent has been otherwise granted by the administrator of information systems management services for the PIP application.

*NOTE: This language is generally required by software licensors.*

3. User Organization Responsibilities

Each User Organization will be responsible for the following:

- (a) to manage and be responsible for all Users and user IDs authorized by the User Organization. This will include:
  - (a) determining who is to have permission to collect and use PIP Data, and the appropriate role for each User; and
  - (b) advising eHealth as soon as possible of any User who no longer requires permission to collect and use PIP Data, who has been terminated or who



may pose a security risk. It is important that eHealth is advised as soon as possible so that appropriate steps may be taken to disable the User's user ID;

- (b) to facilitate any training recommended by the Ministry within the User Organization;
- (c) to assist with the implementation within the User Organization of any security guidelines or user procedures associated with the PIP application provided to the User Organization in writing or by email from the Ministry;
- (d) to ensure appropriate safeguards are in place within the User Organization to protect the PIP Data, as required by *HIPA*;
- (e) to advise the Ministry if the User Organization becomes aware of or reasonably suspects that there has been a security or confidentiality breach, or if a patient or other individual has raised a privacy or security concern with respect to the PIP application; and
- (f) to grant representatives of the Ministry reasonable access to any end-user system, which access includes without limitation both physical access and electronic access via telecommunications or other network connection, for the purpose of managing the application and monitoring/auditing access and use. The User Organization understands that the Ministry may monitor the collection and use of PIP Data and the use of the PIP application by users within the User Organization.

#### 4. eHealth Responsibilities

eHealth agrees to be responsible for the following:

- (a) providing the eHealth Services to the User Organization;
- (b) maintaining all PIP Data in strict confidence;
- (c) using the PIP Data only for the following purposes:
  - (i) use or disclosure of the PIP Data to the extent necessary to provide the eHealth Services (e.g. accessing the PIP Data for the purposes of de-identifying the information or making data corrections);
  - (ii) any other purpose authorized in writing by the Ministry.
- (d) to ensure appropriate and reasonable safeguards are in place to protect the PIP Data when it is within systems or networks within eHealth's control.

#### 5. Disclaimer and Limitation of Liability

- (a) eHealth will take reasonable steps to maintain the availability of PIP and eHealth Services, and will ensure PIP contains reasonable safeguards to protect the accuracy and integrity of the PIP Data.
- (b) Except as described in section 5(a), the eHealth Services, as well as PIP and other eHealth-provided applications accessible by the User Organizations are provided on an “as is” and “as available” basis. There is no warranty or guarantee that the eHealth Services or PIP will be available, or that the PIP Data contained therein will be accurate or complete. It is expressly recognized that the PIP Data may be incomplete and should be reviewed with subject patients for completeness and accuracy by the User Organizations and their authorized Users;
- (c) Use of PIP and the PIP Data is at the User Organization’s sole risk and is in no way intended to replace or be a substitute for professional judgment;
- (d) Except as described in section 5(a), the Ministry makes no representation or warranty, express or implied, as to the operation of the PIP application or eHealth Services, and assumes no legal liability or responsibility for the provision of eHealth Services or the accuracy, completeness or usefulness of any information provided through the PIP application;
- (e) In no event will any past or present Minister of Health, eHealth, the Ministry or their employees, contractors or agents be liable for any special indirect or consequential damages for any act or omission, regardless of whether the action for such damages is brought in tort, including without limitation negligence and contract including without limitation fundamental breach.

6. Security Notice

eHealth may monitor access to PIP to protect the PIP Data and security of PIP. By accessing PIP the User Organizations and the Users are expressly consenting to these monitoring activities.

7. Termination

- (a) eHealth may terminate a User Organization’s access to the eHealth Services:
  - (i) without cause upon 90 days prior written notice; or
  - (ii) immediately upon material breach of this Schedule or the Policy by the User Organization;
- (b) The Ministry may terminate the eHealth Services:
  - (i) without cause upon 90 days prior written notice; or
  - (ii) immediately upon material breach of this Schedule or the Policy by eHealth.

**SCHEDULE C**  
**BORDER COMMUNITY USER ORGANIZATIONS**

As a condition to allowing the Border Community User Organization's Users to use the PIP application, the Border Community User Organization agrees to abide by and be legally bound by the terms and conditions in the PIP Joint Service & Access Policy (the "Policy") supplemented and amended as follows:

(1) **Definitions**

Terms defined in the Policy will have the same definition where used in this Supplement unless expressly otherwise stated.

(2) **Authority**

The Border Community User Organization represents it is properly registered and licensed within its jurisdiction and authorized to collect, use and disclose personal health information as a custodian under the *Health Information Act* (Alberta) or as a trustee under the *Personal Health Information Act* (Manitoba), as applicable.

The Border Community User Organization also represents it has the authority to collect and use the personal health information in the PIP application and that only licensed and duly qualified healthcare professionals will be authorized to access the PIP application.

(3) **Disclosure and Implied Consent**

- (a) The disclosure of information by the Ministry to the Border Community User Organization will be a trustee to non-trustee disclosure as contemplated in section 21 of *The Health Information Protection Act* (Saskatchewan) ("HIPA").
- (b) The Border Community User Organization acknowledges and agrees that the information is being disclosed by the Ministry to the Border Community User Organization on an implied consent basis for the sole purpose of providing a healthcare service for the individual to whom the information relates.
- (c) The Border Community User Organization agrees it is responsible for communicating, obtaining and managing the individual's consent and agrees to respect, support and comply with all patient control mechanisms included within the PIP application.

(4) **Applicable Laws**

- (a) The Border Community User Organization agrees it will comply with:
  - i. all federal and provincial privacy and other laws applicable to its profession, practice, facility or organization ("Applicable Laws"); and

- ii. where applicable, all bylaws and ethical guidelines applicable to its profession or practice.
- (b) For the purposes of the Border Community User Organization's access to PIP under this Supplement, all references to HIPA in the Policy (other than those referring to a trustee-to-non-trustee disclosure under HIPA s. 21) will be replaced with a reference to all Applicable Laws as defined in section (4)(a)(i) above.

(5) **General**

- (a) This Schedule may be amended by the Ministry on the same terms applicable to an amendment to the Policy.