Subject/Title: ***EHEALTH EHR VIEWER AND INTEGRATION JOINT SERVICES/ACCESS POLICY*** (Data Access Agreement)	**Reference Number:** **Effective Date:** ◆, 2013
Approving Authority: **eHealth Saskatchewan ("eHealth")** **Title:** Chief Executive Officer _____ Signature	**Revision Dates:**

NOTES:

1. Prior to eHealth or the Ministry disclosing personal health information to an authorized provider organization ("APO"), the APO must agree, in writing, to comply with and to be legally bound by the provisions of this Policy. Each APO will be given a copy of or access to this Policy.

2. Prior to an individual who is employed by or associated with an APO and who has been authorized to access the EHR Viewer or Integration (a "User") accessing the personal health information, the User must be:

    - Approved by a designated approver appointed by the APO;
    - Agree electronically to comply with and to be legally bound by the provisions of this Policy; and
    - Given a copy of or access to this Policy.

1. High Level Policy

The identifiable information that can be viewed through the EHR Initiative (either through the EHR Viewer or a system-to-system EHR Integration) constitutes personal health information and is subject to the provisions of *The Public Health Act, 1994*, *The Health Information Protection Act*, other provincial legislation as mentioned below, and in some cases federal privacy laws such as the *Personal Information Protection and Electronic Documents Act.*

The collection and use of the personal health information within the EHR Viewer or Integration is restricted to only the Authorized Health Purpose as described in this Policy. The Authorized Health Purpose for the EHR Initiative is to support or provide care to the patient to whom the information relates. Collection, use or disclosure for any other purpose is strictly prohibited. Please see section 9 of this Policy for consequences relating to unauthorized collection, use or disclosure.

This Policy is also intended to act as a data access agreement as discussed below.

This Policy constitutes the entire agreement between eHealth and the APO with respect to the subject matter hereof and supersedes all prior agreements and understandings, oral or written, between the parties with respect to the subject matter hereof.

2. Interpretation

Please see Schedule "A" to this policy for a Glossary of Terms and Acronyms.

3. Scope/Purpose

This Policy applies to:

(a) all APOs who receive EHR Data through the EHR Viewer or Integration; and

(b) all healthcare providers employed or contracted by the APOs who are approved by the APOs to collect, use and disclose the EHR Data from the EHR Viewer or Integration ("Users").

By signing on to the EHR Viewer, or collecting EHR Data through an EHR Integration, an APO's Users are able to view confidential personal health information from the Source Systems (such as PIP, SLRR). As a condition to allowing the APO's Users to sign on to the EHR Viewer or other system that is receiving EHR Data through an EHR Integration, each APO and all Users agree to abide by and be legally bound by this Policy.

This Policy shall act as a data access/sharing agreement, setting out responsibilities and rules of collection, use and disclosure for APOs and Users who are accessing or receiving personal health information from the Source Systems through the EHR Viewer or Integration.

Data sharing with Source Trustees (i.e. the Ministry, RHAs) is excluded from the Policy and is dealt with through Master Data Sharing Agreements with eHealth.

EHR Data and systems will be added to the Policy by the addition of new schedules describing the system, the data, and any other special terms and conditions ("Schedules").

4. Legislative Authority

The Health Information Protection Act (Saskatchewan) ("HIPA")

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

The Prescription Drugs Act (Saskatchewan) – for PIP Data (medication profile)

The Prescription Drugs Regulations, 1993 (Saskatchewan) – for PIP Data (medication profile)

The Public Health Act, 1994 (Saskatchewan) – for SIMS Data (immunization information)

Please see the reference materials at the Ministry of Health website www.health.gov.sk.ca/privacy-statement and the Saskatchewan Office of the Information and Privacy Commissioner ("OIPC") website at www.oipc.sk.ca for further information regarding HIPA.

5. Detailed Policy

5.1 **Accountability**.

5.1.1 Trustee

eHealth is the trustee under *The Health Information Protection Act* (Saskatchewan) ("HIPA") for the EHR Data with the exception of PIP. The Ministry is the trustee under HIPA for PIP. As trustee, eHealth (the Ministry as trustee for PIP) will have custody and control of and make decisions regarding the use and disclosure of the EHR Data.

eHealth (the Ministry for PIP) shall:

(a) appoint an individual who will be responsible for privacy for its EHR Data; and

(b) with respect to EHR Data within its custody or control or within systems within its custody or control, pursuant to section 16 of HIPA, establish 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 access to or use, disclosure or modification of the information; and

(iii) otherwise ensure compliance with HIPA by its employees; and

(c) comply with all applicable laws including, without limitation, HIPA. It is important to note that the OIPC 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."[1]

In other words, the OIPC requires that trustees meet their general duties under HIPA, including as required under sections 9 (right to be informed), 10 (right to information about disclosures without consent), 16 (duty to protect), 19 (duty to collect accurate information), and 23 (collection, use and disclosure on a need-to-know basis) as a condition to relying on the consent provisions outlined in HIPA.

It is the responsibility of eHealth (the Ministry for PIP) to ensure it has the authority to collect, use and disclose the EHR Data as outlined in this Policy.

5.1.2 APO Responsibilities

Each APO shall:

(a) ensure it has a privacy officer appointed for its organization and advise eHealth of:

(i) the individual's name and contact information; and

(ii) any changes to the privacy officer's contact information.

If the APO does not advise eHealth of its privacy officer, the Authorized Approver will be identified as the contact person for privacy issues;

(b) appoint an Authorized Approver who will be responsible to manage and designate Users and User roles for the APO. Where approved by eHealth and the APO, the APO may have multiple Authorized Approvers;

(c) provide eHealth with the contact information for its Authorized Approver and advise eHealth of any changes to the Authorized Approver's contact information;

(d) with respect to EHR Data within its custody or control or within systems within its custody or control, pursuant to section 16 of HIPA, establish policies and procedures to maintain administrative, technical and physical safeguards that will:

(i) protect the integrity, accuracy and confidentiality of the information;

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

(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 access to or use, disclosure or modification of the information; and

(iii) otherwise ensure compliance with HIPA by its employees;

(e) comply with all applicable laws including, without limitation, HIPA and, where applicable, PIPEDA. It is important to note that the OIPC 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."[2]

In other words, the OIPC requires that trustees meet their general duties under HIPA, including as required under sections 9 (right to be informed), 10 (right to information about disclosures without consent), 16 (duty to protect), 19 (duty to collect accurate information), and 23 (collection, use and disclosure on a need-to-know basis) as a condition to relying on the consent provisions outlined in HIPA.

(f) be responsible for all Users authorized by the Authorized Approver and all of their actions and omissions of the Authorized Approver and all Users authorized by the Authorized Approver;

(g) be responsible to ensure all Users authorized by the Authorized Approver have completed all necessary training relating to the EHR Viewer or Integration and have completed appropriate privacy and security training;

(h) be responsible to ensure all Users accessing personal health information in the EHR Viewer have signed a confidentiality oath or agreement; and

(i) be responsible for all acts or omissions of the APO's employees, agents and contractors.

It is the responsibility of each APO to ensure they have authority and consent to collect and use EHR Data as outlined in this Policy.

As part of the sign-up process for access to the EHR Viewer, APOs will be required to complete eHealth's standard Privacy and Security Checklist. eHealth will be relying on the APO's answers to the questions in the Checklist as part of the criteria to determine whether the APO will be granted access to the EHR Data.

[2] Saskatchewan Office of the Information and Privacy Commissioner Investigation Report H-2005-002, Prevention Program for Cervical Cancer at p. 80

5.1.3 Collection and Use of EHR Data

Access by Users to/use of the EHR Data through the EHR Viewer or Integration will include "view and print only" and will be based on the user role and access privileges assigned to each User.

Once the EHR Data has been incorporated into the APO's records this Policy will no longer apply because in such event:

(a) Section 20 of HIPA will apply to all APOs 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 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 EHR Data for a patient and places it within the APO's medical record for the patient, the APO will be subject to the same duties with respect to that information as eHealth and will be expected to comply with HIPA.

(b) Section 21 of HIPA will apply to APOs who are not included as trustees under HIPA but who are accessing the EHR Viewer. 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 APO is a non-trustee (such as an out-of-province physician not licensed to practice in Saskatchewan located in a border community who provides services to a significant number of Saskatchewan residents), it specifically acknowledges that the EHR Data must not be used or disclosed for any purpose other than for an authorized health purpose as described in section 5.2 of this Policy and the APO has the consent of the subject individual. All non-trustee APOs that will be set up to access the EHR Viewer must be specifically approved in writing by eHealth. For further clarification, eHealth may have preconditions that need to be met prior to allowing a non-trustee to access EHR Data.

If HIPA does not apply to the APO, then that APO will be required to protect the confidentiality and security of the EHR Data to the same standard as outlined in this Policy and laws applicable to it.

Each APO will be responsible for designating Users within their organization who will be entitled to collect, use and disclose the EHR Data through the EHR Viewer or Integration. Each APO accepts responsibility for ensuring that its authorized Users comply with this Policy and do not improperly access or use the EHR Data.

5.2 **Identifying Purposes**. The EHR Data shall be collected and used through the EHR Viewer or Integration only for the purpose of supporting or providing care to the patient to whom the information relates and to whom the APO is providing current health services (the "Authorized Health Purpose").

Collection or use of the EHR Data through the EHR Viewer or Integration for any other purpose must be pre-approved in writing by eHealth (the Ministry for PIP).

5.3 **Consent.** The EHR Data is to be collected and used by APOs only for the primary purpose of providing and supporting a healthcare service for the individual to whom the information relates.

The issue of consent and communication with patients is one that always needs to be addressed by the individual healthcare provider with the individual patient.

eHealth recommends APOs use implied or express consent rather than deemed consent as set out in HIPA. eHealth will support the APO's and healthcare providers use of implied consent as follows:

- Ensure brochures and other communication materials are available for the APOs;
- Have information available for patients via the eHealth web-site;
- Answer questions from patients or healthcare providers by providing telephone support. Contact information is as follows:

Mail: eHealth Privacy Service
Suite 360, 10 Research Drive

Regina, SK S4S 7J7

Phone: 1-800-667-1672

Email: PrivacyandAccess@eHealthsask.ca

Fax: (306) 798-0897

- Offer patient control mechanisms to patients to restrict access to their EHR Data. Current patient control mechanisms include:

    - Full Block – this allows the patient to prevent any access to their EHR Data through the EHR Integration or EHR Viewer.

    - Masking – this allows the patient to mask their EHR Data. A User can unmask the EHR Data where the patient expressly consents, in emergency circumstances, etc.

In addition, on request from an individual, eHealth will provide a report to the individual showing who has viewed their information in the EHR Viewer.

eHealth (the Ministry for PIP) and the APOs agree to perform their responsibilities outlined in the communications plan described in Schedule "B" to this Policy.

All requests by a patient to access the patient control mechanisms described in Schedule "B" will be referred to the eHealth Privacy Service. The eHealth Privacy Service agrees to follow the procedures described in Schedule "B" when a patient requests patient control.

Use of the EHR Data is to be done on an express or implied consent basis and all Users agree to respect any patient control mechanisms selected by the patient and displayed in the EHR Viewer or Integration.

5.4 **Limiting Collection and Use.** The APOs and their authorized Users may only collect and use EHR Data from the EHR Viewer or Integration on a need-to-know basis for the Authorized Health Purpose as per section 5.2. The need-to-know must be supported by the User's relationship to the patient and the specific health services being provided. The APOs shall respect the user roles defined within the EHR Viewer or Integration.

5.5 **Accuracy.** If an APO or User becomes aware of any inaccurate or potentially inaccurate information, they shall advise eHealth and, if possible, the applicable Source Trustee.

5.6 **Safeguards.** Each APO agrees that appropriate physical, organizational and technological measures as outlined in section 5.1 will be put in place within their organization to protect the security and confidentiality of the EHR Data and to ensure that this data is only used on a need-to-know basis for the Authorized Health Purpose as per section 5.2.

Each APO agrees to follow any security procedures recommended and approved by eHealth (or the Ministry as it relates to PIP) from time to time.

5.7 **Openness.** The APOs will ensure that their privacy and security policies and procedures are reasonably available to the public on request, and that patients are informed of the anticipated collection and use of their personal health information through the EHR Viewer and Integration. eHealth will support this activity by making the material described in Schedule "B" to this Policy available to APOs.

5.8 **Individual Access/Amendment.** eHealth (the Ministry for PIP) agrees to reasonably address requests for a patient's access to his or her EHR Data and to take reasonable steps to verify the patient's identity before providing a patient with access to his or her EHR Data. Most APOs will have access to a print function. If they do not, they will refer the patient to the eHealth Privacy Service.

Each APO agrees to have appropriate and reasonable policies, procedures and forms in place to facilitate access and amendment, if necessary, by a patient to his or her EHR Data distributed by the EHR Viewer or Integration. Each APO recognizes the importance of providing patients timely access to their EHR Data.

5.9 **Complaints.** All privacy-related complaints relating to the EHR Viewer or Integration will be directed to the eHealth Privacy Service for investigation, review and resolution.

eHealth is authorized to share non-identifying information about complaints received or investigated by eHealth with the Ministry of Health and the RHAs.

Each APO agrees to have appropriate and reasonable policies, procedures and forms to address privacy concerns, complaints or incidents, whether raised by patients or otherwise. For assistance in developing policies and procedures for responding to complaints or incidents, please see the Privacy Breach Guidelines at www.oipc.sk.ca.

Any complaints may be forwarded by the patient to the Saskatchewan Office of the Information and Privacy Commissioner ("OIPC").

5.10 **Audits.** Access to the EHR Data through the EHR Viewer or Integration will be tracked and logged to protect against inappropriate or improper access or use. Details relating to audit outcomes, reporting and review, including the eHealth Privacy Service's role in:

(a) addressing patient requests for audits of access to their personal health information through the EHR Viewer or Integration; and

(b) addressing requests from APOs for audit logs of their Users;

will be determined by eHealth in its sole discretion.

5.11 **Overriding Provision.** Nothing in this Policy is intended to be inconsistent with or contrary to any applicable laws or the rights and duties of eHealth (or the Ministry as it relates to PIP) or the APOs under applicable laws.

6. Procedures/Policies

6.1 **Implementation.** This Policy will be implemented as follows:

(a) Prior to eHealth or the Ministry disclosing personal health information to an APO, the APO must agree, in writing, to comply with and to be legally bound by the provisions of this Policy. Each APO will be given a copy of or access to this Policy.

(b) Prior to a User accessing personal health information in the EHR Viewer, the User must:

(i) Be approved by a designated approver appointed by the APO;

(ii) Be given a copy of or access to this Policy;

(iii) Agree electronically to comply with and to be legally bound by the provisions of this Policy; and

(iv) Sign the confidentiality oath or agreement provided by or approved by the APO.

(c) When logging onto the application, Users will be reminded of the confidential nature of the information and that their access to it is subject to their compliance with this Policy.

6.2 **Addition or Amendment.** eHealth may, at any time, amend the main body of this Policy or Schedules "A" or "B", or add additional Schedules.

Each addition or amendment will become binding on the APOs and their Users upon electronic acceptance, using the following process:

(a) an electronic copy of each addition or amendment will be made accessible to each APO and will be made generally available in the same manner as this Policy; and

(b) each User, when signing onto the EHR Viewer or Integration for the first time after the addition or amendment becomes effective, will be required to electronically agree to the addition or amendment. The text of the addition or amendment will be presented and the User will be required to click "I Accept" before being granted access to the EHR Viewer or Integration.

6.3 **Additional Policies & Procedures.** In addition to the obligations outlined in this Policy, all Users and APOs will be and remain bound to:

(a) comply with all applicable laws including, without limitation, HIPA and, where applicable, PIPEDA;

(b) comply with all applicable ethical requirements and guidelines;

(c) comply with all additional policies, procedures and manuals approved by eHealth and connected to the APOs from time to time; and

(d) comply with all other applicable policies and procedures related to their collection and use of personal health information which may be engaged by their access to the EHR Viewer or Integration.

7. Terms and Conditions of eHealth Services

7.1 Restrictions on Use and Disclosure of the Viewer Object Code. Each APO agrees:

(a) that, to the extent third party code is accessed or used, the APO 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 eHealth and the APO uses with its own confidential information;

(b) to take all reasonable steps to prohibit, and to cooperate with eHealth 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 authorized Users who have a need to know and agree to access the third party code only for that purpose.

NOTE: This language is generally required by software licensors.

7.2 Disclaimer and Limitation of Liability

(a) eHealth will take reasonable steps to maintain the availability of the EHR Viewer and Integration and eHealth Services, to ensure the EHR Viewer and Integration contains reasonable safeguards to protect the accuracy and integrity of the EHR Data, and to accurately present the EHR Data in the EHR Viewer and Integration.

(b) Except as described in section 5(a), the eHealth Services, as well as the EHR Viewer and Integration, and other eHealth provided applications accessible by the APOs are provided on an "as is" and "as available" basis. There is no warranty or guarantee that the eHealth Services, the EHR Viewer or Integration will be available, or that the EHR Data contained therein will be accurate or complete. It is expressly recognized that the EHR Data may be incomplete and should be reviewed with subject patients for completeness and accuracy by the APOs and their authorized Users.

(c) Use of the EHR Viewer and Integration and the EHR Data is at the APO's sole risk and is in no way intended to replace or be a substitute for professional judgment.

(d) Subject to section 7.2(e), in no event will any past or present Minister of Health, eHealth, Source Trustee 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.

(e) Nothing in section 7.2(d) shall relieve eHealth, the Ministry or the Source Trustees from any damages owing as a result of inaccurate EHR Data being provided to the APO where eHealth, the Ministry or the Source Trustee would otherwise be liable at law.

7.3 **Security Notice.** eHealth may monitor access to the EHR Viewer and Integration to protect the EHR Data and security of the EHR Viewer and Integration. By accessing the EHR Viewer or Integration, the APOs and the Users are expressly consenting to these monitoring activities.

8. Term/Termination/Withdrawal

8.1 **Term of Policy.** This Policy shall come into force on the date on which it is approved by the eHealth, and shall remain in force until terminated in accordance with this Article.

8.2 **Withdrawal by APO.** An APO may withdraw from this Policy and from further involvement with or access to the EHR Viewer or Integration by providing 30 days' notice in writing to eHealth.

8.3 **Suspension or Termination of Rights.** If eHealth believes that a User or APO has not complied with the privacy laws applicable to it or with the terms of this Policy, eHealth may, without prior notice, suspend the User/APO's right to collect or use EHR Data in whole or in part.

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

8.4 **Termination by eHealth or the Ministry.** eHealth and the Ministry reserve the right, in their sole discretion and upon 6 months' written notice, to terminate an APO's or User's access right to EHR Data.

9 Enforcement

9.1 **Inappropriate Use**. If eHealth is aware of or suspects improper use, eHealth will follow its Information Incident Management Policy and Process. This may include taking the following actions:

- Investigation;

- Suspension or termination of the User's or APO's access to eHealth's systems;
- Reporting of the User's actions to:
    - the Ministry;
    - the APO;
    - the police, if criminal activity is suspected; and/or
    - the Office of the Information and Privacy Commissioner (Saskatchewan);
- Reporting the User's or APO's action to the appropriate RHA(s) and the appropriate College or other regulatory authority; and/or
- Advising the patient of the incident and advising the patient of their corresponding rights.

9.2 **Breach of Contract**. A breach of this Policy may result in significant legal liability for breach of contract for both the User and the APO.

9.3 **Disciplinary Action**. Any User engaging in conduct inconsistent with this Policy may be subject to disciplinary action from their employer, up to and including termination of employment or service (as appropriate).

9.4 **Criminal Sanctions**. In addition, eHealth or any User or APO who breaches HIPA or any other applicable laws (example: knowingly contravenes any provision of HIPA or the HIPA Regulations) is guilty of an offence pursuant to section 64 of HIPA (**penalties up to maximum $50,000 fine and 1 year imprisonment**) or the enforcement provisions of other applicable laws and is liable on summary conviction.

9.5 **OIPC Investigation**. From time to time, the OIPC may carry out investigations with respect to personal health information in the custody and control of the Users, APOs or eHealth to ensure compliance with HIPA.

SCHEDULE "A"
GLOSSARY OF TERMS AND ACRONYMS

"APO"	means authorized provider organizations approved by eHealth (the Ministry for PIP) to access or receive EHR Data, such as physician offices;
"APO Systems"	means the systems and applications within the control of the APO or its service provider;
"Authorized Approver"	means the person who is authorized to designate Users and User roles for an APO;
"eHealth"	means eHealth Saskatchewan (formerly known as the Saskatchewan Health Information Network), the Treasury Board Crown Corporation which holds the licenses and contracts associated with the administration and management of the EHR Viewer and Integration;
"EHR Data"	means the personal health information included within the EHR Initiative, including without limitation SLRR Data and PIP Data. Additional data may be added from time to time.
"EHR Initiative"	means the electronic health record initiative undertaken by the Province of Saskatchewan through eHealth;
"EHR Integration"	means the system to system integration transferring EHR Data from an eHealth system to an APO System. This is a disclosure by eHealth (the Ministry for PIP) to the APO as per section 20 or 21 of HIPA;
"EHR Viewer"	means the web-based viewer allowing a User to access EHR Data. This is a disclosure by eHealth (the Ministry for PIP) to the APO;
"eHealth Privacy Service"	means the service operated by eHealth 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 EHR Data;
"eHealth Systems"	means systems and applications within the control of eHealth, including the eHealth EHR Viewer and Integration;
"healthcare provider"	means a health professional or an authorized employee who is employed or contracted by an APO. The term "contracted by" means the healthcare provider is not employed but is providing contract services;
"HIPA"	means *The Health Information Protection Act* (Saskatchewan);
"Laboratory Test Results"	means the report captured within an RHA's/SDCL's LIS reporting the results of a laboratory test conducted by or on behalf of the RHA/SDCL for a patient;

"LIS"	means the local Laboratory Information System operated by the Source Trustee;
"Ministry"	means the Saskatchewan Ministry of Health;
"OIPC"	means the Office of the Information and Privacy Commissioner (Saskatchewan);
"patient"	means an individual who is or will be obtaining a health service from an APO;
"personal health information" (as per section 2(m) of HIPA)	means, with respect of 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;
"PIP"	means the Pharmaceutical Information Program;
"PIP Data"	means the dispensed drug information, allergy information, and other information available through PIP;
"PIPEDA"	means the federal *Personal Information Protection and Electronic Documents Act*;
"RHAs"	means the Regional Health Authorities established pursuant to *The Regional Health Services Act* (Saskatchewan);
"SDCL"	means the Saskatchewan Disease Control Laboratory, a branch of the Ministry established under section 8 of *The Department of Health Act* (Saskatchewan);
"SIMS"	means the Saskatchewan Immunization and Management System;
"SIMS Data"	means the data collected, distributed and/or stored in connection with SIMS including a patient's immunization record and associated information;
"SLRR"	means the Saskatchewan Laboratory Results Repository;
"SLRR Data "	means the data collected, distributed and/or stored in connection with SLRR including registration information about patients (HSN, name, etc.) and Laboratory Test Results;

"Source System"	means PIP, SLRR or any other repository that may be added to the EHR Viewer or Integration in the future through a Source System Schedule;
"Source System Schedule"	means the Schedule to this Policy outlining the requirements of a Source System;
"Source Trustees"	means the trustees who are the source of the EHR Data;
"trustee"	means a trustee as defined in HIPA; and
"User"	means an individual who is employed by or associated with an APO who has been authorized to access the EHR Viewer or Integration.

SCHEDULE "B"
COMMUNICATION PLAN AND MATERIALS
AND PATIENT CONTROL PROCEDURES

Patient communication materials have been developed for EHR Viewer and can be found at:

- ***NTD: Add links.***

The APO agrees to make all patient brochures and communication materials available at the links above reasonably available to their patients.

All patient inquiries regarding patient control (masking) or requests for access reports should be directed to the eHealth Privacy Service at:

Mail: eHealth Privacy Service
Suite 360, 10 Research Drive
Regina, SK S4S 7J7

Phone: 1-800-667-1672

Email: PrivacyandAccess@eHealthsask.ca

Fax: (306) 798-0897

SCHEDULE "C"
PHARMACEUTICAL INFORMATION PROGRAM ("PIP")

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 *The Health Information Protection Act* (Sask), the Ministry is the trustee of this information.

The Ministry will be disclosing PIP Data from PIP to authorized provider organizations through the Electronic Health Record Viewer or Integration for the purposes of providing or supporting a healthcare service for the subject individual.

THIS SCHEDULE and this Joint Services/Access Policy, to the extent that it applies to PIP, has been approved on behalf of the Ministry by the hands of its duly authorized signing officer on this _____ day of _____, _____.

Saskatchewan Ministry of Health

Per:_____
Printed Name:

Title: Chief Privacy and Access Officer, Risk and Relationship Management Branch.

Per:_____
Printed Name:

Title: Executive Director, Drug Plan and Extended Benefits Branch.

SCHEDULE "D"
EHR DATA

NOTE: The information included within the EHR Initiative is incomplete. Please see detailed notes and disclaimer on each tab within the EHR Viewer or limitation communications to the APOs as part of an EHR Integration. Please see the communication material referred to in Schedule "B" for more details regarding each data set.

1. SLRR Data

Profile of laboratory test results from SDCL's and participating RHA's LIS systems.

2. PIP Data

Profile of prescription drugs dispensed from participating private pharmacies. See Schedule "C" for further details regarding PIP Data.

3. Clinical Document Repository

This includes clinical documents such as discharge summaries included in the EHR Data. Currently this will include discharge summaries from the RHAs (starting with the Saskatoon Health Region).

4. Saskatchewan Immunization and Management System ("SIMS")

Profile of immunizations received by the individual as entered by participating RHAs.

This section 4 of Schedule "D" applies to immunization data included within the EHR Initiative. This section 4 of this Schedule "D" is intended to override the provisions of the Joint Services/Access Policy as it relates to immunization information only.

The immunization data is being provided by the RHAs and the Northern Inter-Tribal Health Authority ("NITHA") pursuant to a Data Sharing Agreement. Under the Data Sharing Agreement, the RHAs and NITHA have approved the inclusion of the immunization data within the EHR Initiative. eHealth may only use and disclose the immunization data in accordance with the approval and APOs may only use and disclose the immunization data in accordance with the Joint Services/Access Policy.

5. Chronic Disease Management – Quality Improvement Program ("CDM-QIP")

If you are a Physician participating in the CDM-QIP Program, please see the Clinical Best Practices at www.heatlh.gov.sk.ca/cdm-qip regarding the completion of the CDM-QIP templates and forms.