



Privacy Policies and Procedures - Template for the Pharmacy

Contents

Forward	2
Section 1.....	2
Privacy Laws – Protection of Personal Health Information	2
A. Definitions	2
B. Resources	5
C. Policy	6
D. Employee Privacy Pledge.....	9
E. Addendum.....	10
Section 2.....	11
Attachments.....	11
A. Saskatchewan College of Pharmacy Professionals, “Patient Confidentiality and the Release of Confidential Records,” November 2016.....	11
B. Saskatchewan College of Pharmacy Professionals, “Policy Statement for Pharmacists and Pharmacy Technicians: Accessing Patient-Specific Information from the Medication Profile Viewer (MPV) Available Under the Pharmaceutical Information Program (PIP)”, November 2016:.....	13
C. Saskatchewan College of Pharmacy Professionals, “Guidelines for Pharmacists and Pharmacy Technicians: Accessing Patient-Specific Information from the Medication Profile View (MPV) Available under the Pharmaceutical Information Program (PIP)”, October 2016:.....	16
E. <i>The Pharmacy and Pharmacy Disciplines Act, 2015</i>	21
F. The Pharmaceutical Information Program (PIP):	22

Forward

[This Pharmacy] has instituted policy and practice guidelines to meet the requirements of and ensure compliance with *The Health Information Protection Act* as amended by *The Statutes of Saskatchewan 2008*.

This document is to accompany and enhance existing policy at [this pharmacy]. It does not replace or discount any policy or practice guidelines set out by the Saskatchewan College of Pharmacy Professionals, nor any laws of the Province of Saskatchewan and the Government of Canada.

This document contains guidelines for pharmacy practice and is intended for strict adherence by pharmacists, pharmacy technicians, dispensary assistants and all students and other individuals providing pharmacy care to the clients of [this pharmacy]. Further, this document will guide the practice of all staff members of [this pharmacy] – it is acknowledged that in the normal course of duty, administrative staff, delivery staff, clerks and other personnel will overhear health-related conversations and handle the prescriptions of customers and individuals who patronize this pharmacy to seek health information and other pharmaceutical services.

This policy has been created and endorsed by [the managing partners and staff of this pharmacy] and is agreed upon by the undersigned.

Section 1

Privacy Laws – Protection of Personal Health Information

A. Definitions

Access is the right of the individual (a patient or an authorized representative, such as a tax preparer) to view or obtain copies of information recorded, stored, or otherwise in custody of this pharmacy. NOTE: The right of the individual to access their own health information is governed differently than the discretionary provision of health information to other health providers.

Approver refers to the individual who has the authority to designate pharmacists and pharmacy technicians as having a right to access an individual's pharmaceutical information profile (PIP).

Collect, in reference to health information, is synonymous with "gather, obtain access to, acquire, receive or obtain" by any means.

Commissioner refers to the Information and Privacy Commissioner, appointed pursuant to Section 38 of *The Freedom of Information and Protection of Privacy Act*.

Confidentiality is a term which refers to the protection of personal information, but has nuances which vary according to the particular situation and is **not** to be mistaken as being synonymous with "privacy."

Consent, as pertaining to disclosure of personal health information, is deemed to be an authority held at one of three standards:

1. the highest standard is express consent (required in three particular situations);
 - a) under section 27(2) of HIPA, express consent is deemed to have been provided for the primary purpose of providing health care to the subject individual;
2. the lower standard is implied consent with a right to opt out (used most frequently in the course of duty); and,
3. the no-consent situation (as may be required in an emergency).

The health care provider entrusted with personal health information must weigh the circumstances against ethics and the law to determine which of these standards under which he/she is making a disclosure.

De-identified material refers to any document of prescription item from which any information that may reasonably be expected to identify an individual has been removed.

Disclosure is a term reserved for revealing personal health information to a party outside the realm of operation and control of this pharmacy. Each act of disclosure shall contain the least amount of personal information as required for each particular request.

NOTE: Discussion or exchange of information between staff members, regardless of physical location, would not be regarded as an act of disclosure; nor would informational exchanges with our information management service provider. However, in all such exchanges, staff shall endeavour to safeguard personal information from outside observation.

(The) Health Information Protection Act (HIPA) is the overarching set of laws, created by our Legislature, to govern the collection, storage, use, access and disclosure of Personal Health Information and the Privacy of Individuals with respect to this information (see addendum).

Manager refers to the licensed pharmacist(s) designated by the proprietor(s) of the retail pharmacy to have authority over and be responsible for the operation and whose name(s) appear on the permit.

(The) Pharmacy and Pharmacy Disciplines Act is a legislated set of laws which, amongst other things, governs the functions and work conducted in pharmacies by pharmacists and pharmacy technicians (see addendum).

Privacy is a term which refers to the legally and constitutionally protected right of each citizen to exert control over his/her personal health information. Although the definition is broad and subject to nuances as dictated by each situation and interaction with and among health professionals, the overarching importance of privacy is embedded in an individual's right to life, liberty and security. Therefore, the importance of ensuring the privacy of health information for all individuals, whether customers, potential customers, or employees of this pharmacy, shall be valued as on par with ensuring the rights to life, liberty and security (see addendum).

Privacy breach occurs when there is unauthorized disclosure, viewing or collection of personal health information, regardless of source or format, and regardless of whether this information is revealed to a third party. A privacy breach is deemed also to occur when a trustee (or staff

under his/her supervision) fails to take reasonable precautions to safeguard duly collected personal information from exposure.

Record refers to any information that is recorded or stored by any means, or in any device, including a computer or electronic media.

Saskatchewan College of Pharmacy Professionals is the governing body for pharmacists, pharmacy technicians and proprietary pharmacies operating in the province of Saskatchewan.

Security is the means by which personal health information is held to the expected standard of privacy and safeguarded against inadvertent or intentional observation or collection by a third party.

Trustee refers to of the following that have custody or control of personal health information:

- i. a government institution;
- ii. a regional health authority or a health care organization;
- iii. a person who operates a special-care home;
- iv. a licensee as defined in *The Personal Care Homes Act*;
- v. a proprietor as defined in *The Pharmacy and Pharmacy Disciplines Act*;
- vi. a licensed health care professional, including licensed pharmacists and pharmacy technicians, who are not employees of a trustee.

The trustee for this pharmacy is _____.

B. Resources

1. Innovation, Science, and Economic Development Canada (formerly Industry Canada): <http://www.ic.gc.ca/eic/site/icgc.nsf/eng/home>
2. National Association of Pharmacy Regulatory Authorities (NAPRA), Pharmacy Practice and Regulatory Resources: http://napra.ca/pages/Practice_Resources/default.aspx
3. Office of the Information & Privacy Commissioner of Saskatchewan: <http://www.oipc.sk.ca/>
4. Pharmaceutical Information Program (PIP): <https://www.ehealthsask.ca/services/pip>
5. Saskatchewan College of Pharmacy Professionals: <http://www.saskpharm.ca/>
6. Saskatchewan Office of the Information and Privacy Commissioner, “Best Practices, Mobile Device Security,” May 27, 2009: <http://www.oipc.sk.ca/Resources/Helpful%20Tips%20-%20Best%20Practices%20-%20Mobile%20Device%20Security%20-%20March%202011.pdf>
7. Saskatchewan Office of the Information and Privacy Commissioner, “HIPA & Health Regulatory Bodies – Making it Work,” March 21, 2009. [http://www.skcp.ca/AGM%202009%20Gary%20Dickson%20Q.C.%20Presentation,%20Strategies%20for%20Compliance%20with%20the%20Health%20Information%20Protection%20Act%20\(HIPA\)/Strategies%20for%20Compliance%20with%20the%20Health%20Information%20Protection%20Act%20\(HIPA\).pdf](http://www.skcp.ca/AGM%202009%20Gary%20Dickson%20Q.C.%20Presentation,%20Strategies%20for%20Compliance%20with%20the%20Health%20Information%20Protection%20Act%20(HIPA)/Strategies%20for%20Compliance%20with%20the%20Health%20Information%20Protection%20Act%20(HIPA).pdf)
8. Saskatchewan Office of the Information and Privacy Commissioner, “Investigation Report H-2010-01,” March 23, 2010: <http://www.oipc.sk.ca/Reports/H-2010-001,%20March%2023%202010.pdf>
9. Saskatchewan Office of the Information and Privacy Commissioner, “Predictable Problem Areas for Trustees,” March 21, 2009: [http://www.skcp.ca/AGM%202009%20Gary%20Dickson%20Q.C.%20Presentation,%20Strategies%20for%20Compliance%20with%20the%20Health%20Information%20Protection%20Act%20\(HIPA\)/PREDICTABLE%20PROBLEM%20AREAS%20FOR%20TRUSTEES.pdf](http://www.skcp.ca/AGM%202009%20Gary%20Dickson%20Q.C.%20Presentation,%20Strategies%20for%20Compliance%20with%20the%20Health%20Information%20Protection%20Act%20(HIPA)/PREDICTABLE%20PROBLEM%20AREAS%20FOR%20TRUSTEES.pdf)
10. Saskatchewan Office of the Information and Privacy Commissioner, “Privacy Breach Guidelines: Tips for Public Bodies/Trustees Dealing with Privacy Breaches,” July 2016: <http://www.oipc.sk.ca/Resources/2014-2015/Privacy%20Breach%20Guidelines%20for%20Public%20Bodies%20and%20Trustees.pdf>
11. Saskatchewan Office of the Information and Privacy Commissioner, “Privacy Considerations: Faxing Personal Information and Personal Health Information,” June 4, 2009: <http://www.oipc.sk.ca/What's%20New/Faxing%20PI%20and%20PHI%20Guidelines%20-%20June%204%202009%20-%20FINAL.pdf>
12. *The Health Information Protection Act, 2004*: <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/H0-021.pdf>
13. *The Freedom of Information and Protection of Privacy Act, 1990*: <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf>
14. *The Pharmacy and Pharmacy Disciplines Act, 2015*: <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/P9-1.pdf>

C. Policy

Assuring and Overseeing Privacy Compliance

The [management of this pharmacy] have created this policy statement to ensure that all staff perform their duties in a manner that complies with the highest standards in protecting personal health information. Upon implementation, _____, PIP Approver and Trustee, will be responsible for overseeing privacy compliance as pertaining to the Health Information Protection Act (HIPA) and other pertinent laws and guidelines that apply to pharmacy practice.

Confidentiality Agreements with other Service Providers / Affiliates

The [management of this pharmacy] will endeavour to ascertain that pertinent laws are abided by third parties providing service and support functions. Similarly, any future affiliates will be informed of operational expectations.

Purpose for Use of Personal Information

It is important for all staff members to be cognizant of the particular use for any piece of personal information and that it is used appropriately, ethically, and within all pertinent guidelines. In particular:

- Personal health information may be collected and used for primary (direct) pharmacy services including: dispensing and patient consultation.
- Such information may also be collected to discuss health and pharmacy care with a third party connected with the particular patient. For example, a family member or guardian may have relevant inquiries. It is important to ascertain that all third parties have the appropriate consent from the particular patient.
- Personal information may be required for the purposes of a pharmacy meeting. It is important that only pertinent information be divulged and that this information is discussed only in the presence of authorized and pertinent personnel.

In cases where the policy is not clear, legal advice must be consulted. For more information visit Office of the Saskatchewan Information and Privacy Commissioner website at: <http://www.oipc.sk.ca/>.

Reasonable Notice of Privacy Policy and Practice

This pharmacy has displayed, within easy public access, a number of brochures including the brochures entitled “The Pharmaceutical Information Program”, issued by eHealth Saskatchewan. Staff members are herein encouraged to remain informed of the latest guidelines concerning privacy so that they are able to inform the public.

Safeguarding Personal Information

Personal information must be revealed or discussed in such a manner that other members of the public do not inadvertently become apprised of such. This includes, but is not restricted to the following practices:

- In preparation for dispensing functions, and all areas of pharmaceutical care that may follow, only those staff members who have a reasonable expectation of actively participating in the care of the particular patient and have implied or overt consent to do so (at this or a later time frame) should seek to learn any facts pertinent to this patient.
- In regard to the physical area where counselling occurs, use discretion and common sense in counselling patients on drug use and health issues (in terms of having any conversation overheard by members of the public or uninvolved staff members).
- In counselling patients on any aspect of their care, it is incumbent on each staff member to use all reasonable measures to ensure that members of the public (and staff members with NO reasonable expectation of being actively involved with care at this or a later date) are not inadvertently apprised of confidential information. It is important that each member be cognizant that all information at our disposal concerning all patients must be regarded as confidential. Further, it is important to note that a patient may, at any time or any topic, APPEAR to be completely open with their information, that this information, too, must be regarded and handled with full confidentiality. For example, patients may conduct themselves as though they were carefree about their prescriptions in order to hide deep embarrassment. On the other hand, all patients must be considered as vulnerable in that they are attending at the pharmacy to seek assistance with matters that they cannot handle on their own and that they likely do not have full understanding of.
- Information removed from the premises, such as may be required for use at off-site counselling, meetings, or file review, must be safeguarded from public access.
- All patient information shall be safeguarded in accordance with pharmacy practice laws and guidelines (HIPA). As such, the dispensary shall be treated as a specialized area of the pharmacy premises. In particular, staff members are herein advised that only pertinent staff shall be present in the dispensary. Patients and ancillary staff shall be rerouted when possible and otherwise guided and supervised at all times that they may be within the confines of the dispensary. The dispensary, as for the rest of the premises, shall be safeguarded against access and theft at all times (alarmed during the hours that the pharmacy is not open for business).
- Faxing personal (health) information increases the risk of such information being improperly disclosed or exposed. The most common causes include: misdialing; viewing by an unintended recipient at the other end; or by dialing a number no longer in service. The following guidelines will safeguard against these possibilities:
 - use a pre-programmed speed dialing system whenever possible;
 - double-check all dialed numbers before pressing “send”;
 - when possible, use a cover page that contains a confidentiality warning statement;
 - ensure letterheads are updated when a fax number changes;
 - clear the memory of any fax machine when it is taken out of service;
 - confirm a seldom-employed fax number before sending any information to this number;
 - send only the minimum amount of information required for each purpose;
 - consider a more secure format (mail, telephone conversation, etc.) when possible; and,
 - when a client requests that personal information be sent via fax, ensure they are made aware of the risk of exposure inherent in this transmission format.

Requests for Personal Information

The detailed rules within HIPA and PIPEDA will govern the provision of personal information. In general, such provision shall be open, timely and appropriately presented.

Privacy-related Complaints

All staff members must be aware and ready to act on any complaint related to confidentiality. Whether deemed to be real or perceived in nature, every complaint must be dealt with immediately and in a manner that portrays to the individual our deep concern with issues of privacy (as with all areas of pharmacy care). In particular, a staff pharmacist or pharmacy technician must be summoned immediately so that the matter may be addressed on as personal a basis as possible and handled as deemed appropriate by the pharmacist or pharmacy technician. Further, _____, the trustee, must be immediately notified of the apparent problem to further clarify and address any action that may be required (whether in terms of patient assurance and/or policy amendment).

Assurance that Staff Members are Apprised of and will Abide by Privacy Policy

All members of the pharmacy staff will have read these guidelines and agreed to abide by the rules and intent of these policies, as indicated by their signature on the attached confidentiality form.

D. Employee Privacy Pledge

The confidentiality of the personal information of all clients of [this pharmacy] is a key concern. Accordingly, this pharmacy has policies, procedures and practices in place to assure the protection of all such information. Included in our policy is the requirement for every staff member to sign a confidentiality pledge. Therefore, I, the undersigned, agree as follows:

1. That I will only access personal health information on a need-to-know basis for performing services on behalf of the pharmacy;
2. That I will keep all personal health information in my possession in the strictest of confidence and only use such information for the purposes of performing services on behalf of the pharmacy;
3. That upon no longer requiring the personal health information for the purposes of providing services on behalf of the pharmacy, I will return or destroy all copies of the personal health information in my possession as instructed by the pharmacy manager;
4. That I will follow all applicable pharmacy security, privacy and confidentiality policies, procedures and practices;
5. I acknowledge that I have read and understood this Privacy and Confidentiality Pledge and understand that a breach of it may be in contravention of the *Health Information Protection Act* or other applicable laws.

Name (printed): _____

Position: _____

Signature: _____ Date: _____

Witness: _____ Date: _____

E. Addendum

List of Attachments:

1. Saskatchewan College of Pharmacy Professionals, “ Patient Confidentiality and the Release of Confidential Records,” November 2016
http://scp.in1touch.org/uploaded/web/refmanual/REF_Patient_Confidentiality_&_Release_Confidential_Records_Current.pdf
2. Saskatchewan College of Pharmacy Professionals, “**Policy Statement** for Pharmacists and Pharmacy Technicians: Accessing Patient-Specific Information from the Medication Profile Viewer (MPV) Available Under the Pharmaceutical Information Program (PIP)”, November 2016:
http://scp.in1touch.org/uploaded/web/refmanual/REF_Accessing_PIP_Policy_Current.pdf
3. Saskatchewan College of Pharmacy Professionals, “**Guidelines** for Pharmacists and Pharmacy Technicians: Accessing Patient-Specific Information from the Medication Profile View (MPV) Available Under the Pharmaceutical Information Program (PIP)”, October 2016:
http://scp.in1touch.org/uploaded/web/refmanual/REF_PIP_Pharmacy_Information_Program_Guidelines_Current.pdf
4. *The Health Information Protection Act* (HIPA), 2004
<http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0-021.pdf>
5. *The Pharmacy and Pharmacy Disciplines Act*, 2015
<http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/P9-1.pdf>
6. The Pharmaceutical Information Program (PIP) <https://www.ehealthsask.ca/services/pip>

Section 2

Attachments

A. Saskatchewan College of Pharmacy Professionals, “Patient Confidentiality and the Release of Confidential Records,” November 2016:

http://scp.in1touch.org/uploaded/web/refmanual/REF_Patient_Confidentiality_&_Release_Confidential_Records_Current.pdf

In this document, unless the context indicates otherwise, “member(s)” includes licensed pharmacist(s) and pharmacy technician(s).

The Code of Ethics of the Saskatchewan College of Pharmacy Professionals states that "a member shall protect the patient's right of confidentiality." During the course of practice, members acquire medication and other medical and personal information about their patients. Therefore, the member is ethically obliged to respect the confidential nature of this information.

However, because our Code of Ethics also states that "a member shall hold the health and safety of the public to be a first consideration," "a member shall observe the law," and that "a member shall cooperate with other health care practitioners to ensure delivery of the highest level of pharmaceutical services to the public," it is recognized that this confidential information must be disclosed in certain circumstances, and in other cases, should not be disclosed.

Circumstances when confidential patient information may be disclosed to third parties include:

1. The patient consents to release of the information. Written consent from the patient should be obtained. At a minimum, the member should be satisfied that the patient has expressly permitted the release of the information sought.
2. Release of the information is necessary to comply with the law. For example:
 - a. a police officer presents a warrant
 - b. a member is served with a subpoena which requires delivery of documents containing the patient records
 - c. release of the information is required by Rules of Court that relate to production of information in a law suit
 - d. an inspector authorized to have access to the records under *The Pharmacy and Pharmacy Disciplines Act* makes a request to access the records
 - e. an inspector authorized to have access to the records under *The Controlled Drugs and Substances Act*, or *The Food and Drugs Act* makes a request to access the records pertaining to Narcotic and Controlled Drugs, Benzodiazepines and other Targeted Substances and other drugs respectively
3. Police, other law enforcement agencies or officials, or licensing authorities request the information and the member deems it to be in the best interest of the public to provide such information.
4. Members and other health care professionals for bona fide medical and/or pharmaceutical reasons where, in the judgment of the member, it is prudent to provide this information in the

interests of the patient to protect the mental or physical health or safety of the patient.

5. Release of the information is required to be made to legal counsel for use in providing legal services to the College and/or one or more of its members.
6. Members may disclose to third parties (i.e. a commercial data compiler) prescription information including information concerning the prescriber/member/pharmacy, which does not, and may not reasonably be expected to identify, the patient on the understanding that the third party will not disclose this information with respect to the prescriber/member/pharmacy except in an aggregate format (i.e. which does not disclose specific individual prescribing or dispensing information), without signed consent from the prescriber/member/pharmacy. The onus to obtain this consent is on the third party requesting such information.

Therefore, confidential patient information should not be released without the patient's consent or the consent of others as described above, where legal authority does not exist or in situations where it is not in the interests of the patient or the public at large to provide the information. Where consent is required, it is recommended that the permission be in writing.

Please refer to supplemental guidelines entitled "HIPA and PIPEDA—Preparing Your Community Pharmacy" and "Privacy - Release of Confidential Records of Minors to Parents/Guardians."

B. Saskatchewan College of Pharmacy Professionals, “Policy Statement for Pharmacists and Pharmacy Technicians: Accessing Patient-Specific Information from the Medication Profile Viewer (MPV) Available Under the Pharmaceutical Information Program (PIP)”, November 2016:

http://scp.in1touch.org/uploaded/web/refmanual/REF_Accessing_PIP_Policy_Current.pdf

PREAMBLE

In this policy:

“**pharmacist**” includes pharmacy proprietor; and,

“**privacy legislation**” means the Health Information Protection Act (Saskatchewan) and the Personal Information Protection and Electronic Documents Act (Canada).

PIP has been developed with the primary purpose of improving patient care in Saskatchewan. Via the MPV, PIP provides Saskatchewan pharmacists and pharmacy technicians access through a secure computer network to information about drugs dispensed to Saskatchewan patients in Saskatchewan pharmacies.

Access to information within PIP is provided to pharmacists and pharmacy technicians to assist them to deliver the best possible quality of pharmaceutical care to their patients.

Access, using, or disseminating information from the PIP program, other than as permitted in this policy, is professional or proprietary misconduct.

GENERAL PRINCIPLES

Pharmacists and Pharmacy Technicians:

1. Must be able to justify the reason for accessing information through PIP;
2. Should only access information through PIP when the information that the pharmacist or pharmacy technician expects to obtain may reasonably affect the pharmaceutical care provided to the patient;
3. Should only access the minimum amount of information through PIP that is reasonably required for the purpose for which the information was accessed;
4. Should ensure that only those persons who have a need to know the information should be permitted to access the information;
5. Should only use the information from PIP for the primary purpose of providing pharmaceutical care to their patient, or as is otherwise permitted by privacy legislation or other applicable laws;
6. Should only disclose the information from PIP for the purpose of providing pharmaceutical care to their patient, with the consent of the patient, or as is otherwise permitted by privacy legislation or other applicable laws;

7. Should have appropriate policies and procedures in place to protect the information accessed through PIP from being seen by persons who are not authorized to see that information;
8. Must comply with privacy legislation in connection with the information accessed through PIP; and,
9. Should ensure that persons who the pharmacist or pharmacy technician authorizes to access the information within PIP are aware of and understand their responsibilities.

SPECIFIC REQUIREMENTS

1. Pharmacists or pharmacy technicians will not permit any other person under their authority or control (i.e. a pharmacy assistant) to access the information within the PIP database unless the following conditions are met:
 - a. That person has been specifically authorized by the pharmacist or pharmacy technician to access the PIP database for a purpose for which the pharmacist or pharmacy technician may access the information; and,
 - b. That person has signed a confidentiality agreement in which that person has agreed, among other things, to access the information only on a need-to-know basis, and not to disclose the information to any other person except as permitted by privacy legislation.
2. Pharmacists and pharmacy technicians must report to the PIP, or such other person or organization as may be specified by the PIP, all activities by any individual or entity that the pharmacist or pharmacy technician suspects may compromise the privacy of the patient or confidentiality of confidential information or be a breach of this policy.

MASKING OPTION

PIP provides an option whereby patients can choose to “mask” their drug profiles. Unless unmasking of the drug profile is authorized as provided below, pharmacists and pharmacy technicians are not permitted to access masked drug profiles.

The masking option is administered by Saskatchewan Health or eHealth Saskatchewan. Patients can initiate the masking process by contacting Saskatchewan Health. Pharmacists and pharmacy technicians should be able to provide general information about the masking process to patients upon request.

Pharmacists and pharmacy technicians may only access a masked drug profile in the following circumstances:

1. Expressed consent of the patient has been obtained;
2. In emergency circumstances where the pharmacist or pharmacy technician believes on reasonable grounds that the use or disclosure will avoid or minimize a danger to the health or safety of any person; or,
3. A prescription being filled is on the list of dangerous drugs attached to this policy statement. These are the same drugs as those monitored under the Prescription Review Program

(PRP) pursuant to Regulatory Bylaw 18.1 of the College of Physicians and Surgeons of Saskatchewan.

With respect to the list of dangerous (i.e. PRP) drugs attached, the College is of the view that pharmacists and pharmacy technicians may, upon presentment of a prescription for a PRP drug listed on Appendix A, access the patient's masked drug profile given the inherent risk factors and patient safety issues associated with these drugs. Steps will be taken to specifically advise patients of this unmasking requirement at or near the time the patient applies for masking. As such, the patient need not be proactively advised by the pharmacist or pharmacy technician that his/her drug profile is being accessed in these circumstances. However, if inquiries are made the pharmacist or pharmacy technician should be prepared to advise patients of the unmasking requirement for this list of drugs and that the prescription cannot be filled without access to the drug profile.

C. Saskatchewan College of Pharmacy Professionals, “Guidelines for Pharmacists and Pharmacy Technicians: Accessing Patient-Specific Information from the Medication Profile View (MPV) Available under the Pharmaceutical Information Program (PIP)”, October 2016:

http://scp.in1touch.org/uploaded/web/refmanual/REF_PIP_Pharmacy_Information_Program_Guidelines_Current.pdf

In this document, unless the context indicates otherwise, “member(s)” includes licensed pharmacist(s) and pharmacy technician(s).

1. Definitions

Please see the Glossary of Terms attached as Schedule “A” for the definition of some of the terms used in these guidelines.

2. Accountability

eHealth Saskatchewan is the trustee for the PIP database. Personal health information accessed through the PIP is being shared on a trustee to trustee basis under HIPA. The pharmacy proprietor becomes the trustee for all PIP data accessed by the pharmacy. The pharmacy proprietor is responsible for ensuring that all pharmacists, pharmacy technicians or other persons with access to patient and PIP data within the pharmacy comply with these Guidelines.

3. Purpose

The primary purpose for accessing and using PIP data is to support or provide a health service to the patient to whom the personal health information relates.

Authorized secondary purposes include using and disclosing the PIP data are outlined in the SCPP document “Guidelines for Use and Disclosure of Personal Health Information for Secondary Purposes.”

Care must be taken to ensure only a minimal amount of information is used or disclosed. De-identified information should be used or disclosed if possible. The member must notify the patient in writing if they have relied on emergency circumstance to disclose information.

Reasonable grounds means the member has knowledge of reasonable facts. It does not include a mere suspicion or conclusion based on racial or socio-economic profiling.

4. Patient Control

A member will support and assist patients in using the masking functionality included within PIP. This will include:

- a) providing the patient with a PIP privacy brochure on request and pointing out to the patient the telephone number to call to request a form that allows the patient to implement the masking;
- b) explaining to the patient how masking works.

Members will respect the masking where implemented by the patient. Members may only access a masked drug profile in the following circumstances:

- a) Express consent of the patient has been obtained;
- b) In emergency circumstances where the member believes on reasonable grounds that the use or disclosure will avoid or minimize a danger to the health or safety of any person; or,
- c) A prescription being filled is on the list of dangerous drugs (refer to Appendix A of the corresponding policy statement).

Any requests by a patient to mask or unmask their information will be referred to the PIP Privacy Service.

5. Patient Communication

The member will ensure that PIP Privacy Brochures are readily available to their patients and provide a PIP Privacy Brochure to a patient on request.

The member will also reasonably respond to any direct questions from a patient regarding PIP and will attend PIP training sessions so that they can answer such questions. The member will not be required to answer in depth privacy questions but the member should be able to provide a reasonable overview of PIP. Any detailed questions should be referred to the pharmacy's privacy officer or PIP privacy service.

6. Limiting Use and Disclosure

The member will only use and disclose the PIP data on a need to know basis for the primary purpose of providing health services to the subject individual or for an authorized secondary purpose. The PIP data shall not be accessed, used or disclosed by a member for personal interest, gossip or financial gain.

Access within the pharmacy to the PIP will be limited to authorized users who have been appropriately registered and authorized with the PIP Administration Office.

Saskatchewan Health or eHealth Saskatchewan technical support will be allowed access to the PIP within the pharmacy. Such access should only be allowed after the pharmacy proprietor or pharmacy manager or their designate have taken reasonable steps to confirm the identity of the of the technical support person.

7. Safeguards

The pharmacy manager and the pharmacy proprietor must:

- a) implement the security standards outlined in the PIP Security Standards prior to connecting to the PIP;
- b) implement any changes to the PIP Security Standards when advised to do so by the PIP Administration Office;
- c) ensure all staff and third parties who will access the PIP data have signed a confidentiality undertaking in the form called "Sample Employee Privacy Pledge and

Confidentiality Pledge” attached to the guidelines entitled “Preparing Your Community Pharmacy for HIPA and PIPEDA”; and

- d) ensure reasonable security and confidentiality policies, procedures and practices are in place in compliance with applicable law.

8. Access by Patients

The member will allow their patients to have access to their medication profile except where access to such information may be denied in accordance with applicable law. In other words, the patients will have the same rights of access to their drug profile as they would have access to their other personal health information in the custody and control of the pharmacy. Members will provide a printed or electronic copy of the drug profile to the patient on request.

9. Amendment

Any requests for amendment to a patient’s drug profile will be documented by the member and forwarded to the PIP privacy service for processing. If applicable, the member will also provide their comment as to whether the amendment should be made or not made and any other relevant background information.

10. Complaints

Any complaints relating to a member’s access or use of the PIP Data will be dealt with in the same manner as any other patient complaint. If the complaint relates to how the PIP deals with processes or stores the information (rather than a practitioner’s use or disclosure of the information), the complaint should be referred to the PIP privacy service. Such a complaint should be referred as soon as possible so it can be addressed in an expeditious fashion.

**SCHEDULE “A”
GLOSSARY OF TERMS**

“Act”	means <i>The Pharmacy and Pharmacy Disciplines Act</i>
“Masking” and “Unmask”	means the functionality offered by PIP that allows a patient to globally mask and unmask the prescription drugs in their medication profile
“HIPA”	means the Health Information Protection Act (Saskatchewan)
“medication profile”	means the medication profile of the patient as stored in the PIP database
“personal health information”	means personal health information as defined in HIPA
“Pharmacist”	means a licensed pharmacist as defined in the Act
“Pharmacy Manager”	means a manager as defined in the Act
“Pharmacy Proprietor”	means a pharmacy proprietor as defined in the Act
“Pharmacy”	means a pharmacy as defined in the Act
“Pharmacy Technician”	means a licensed pharmacy technician as defined in the Act
“PIP Data”	means the medication profiles for all patients stored on PIP
“PIP Database”	means the database related to PIP which stores the PIP Data
“PIP Security Standards”	means the PIP Security Standards established from time to time and forwarded out to pharmacies by the trustee of the PIP Database
“trustee”	means a trustee as defined in HIPA

D. *The Health Information Protection Act (HIPA), 2004:*

<http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0-021.pdf>

An Act respecting the Collection, Storage, Use and Disclosure of Personal Health Information, Access to Personal Health Information and the Privacy of Individuals with respect to Personal Health Information and making consequential amendments to other Acts.

WHEREAS the Legislative Assembly recognizes the following principles with respect to personal health information:

THAT personal health information is private and shall be dealt with in a manner that respects the continuing interests of the individuals to whom it relates;

THAT individuals provide personal health information with the expectation of confidentiality and personal privacy;

THAT trustees of personal health information shall protect the confidentiality of the information and the privacy of the individuals to whom it relates;

THAT the primary purpose of the collection, use and disclosure of personal health information is to benefit the individuals to whom it relates;

THAT, wherever possible, the collection, use and disclosure of personal health information shall occur with the consent of the individuals to whom it relates;

THAT personal health information is essential to the provision of health services;

THAT, wherever possible, personal health information shall be collected directly from the individual to whom it relates;

THAT personal health information shall be collected on a need-to-know basis;

THAT individuals shall be able to obtain access to records of their personal health information; THAT the security, accuracy and integrity of personal health information shall be protected;

THAT trustees shall be accountable to individuals with respect to the collection, use, disclosure and exercise of custody and control of personal health information;

THAT trustees shall be open about policies and practices with respect to the collection, use and disclosure of personal health information”.

E. *The Pharmacy and Pharmacy Disciplines Act, 2015:*

[http://scp.in1touch.org/uploaded/web/refmanual/The Pharmacy and Pharmacy Disciplines Act.pdf](http://scp.in1touch.org/uploaded/web/refmanual/The_Pharmacy_and_Pharmacy_Disciplines_Act.pdf)

The Pharmacy and Pharmacy Disciplines Act

being

Chapter P-9.1 of the *Statutes of Saskatchewan, 1996* (effective January 1, 1998) as amended by the *Statutes of Saskatchewan, 1998, c.6; 2002, c.R-8.2; 2003, c.8;*

2009, c.T-23.01; 2010, c.B-12 and c.19; 2014, c.E-13.1 and c.17; and 2015, c.17.

F. The Pharmaceutical Information Program (PIP):

<https://www.ehealthsask.ca/services/pip>

The Pharmaceutical Information Program (PIP) will improve the health of Saskatchewan residents, by providing authorized health care professionals (e.g. pharmacists, pharmacy technicians and physicians) with confidential access to patient medication records. Having access to quality information about their patients will help Saskatchewan health care professionals offer the highest quality of care.

Prior to the introduction of PIP, there was no centralized, complete source of prescription records for health care providers to use when making decisions about a patient's drug therapy. PIP will ensure that individuals and their health care providers have the information needed to make the best decisions about their health care.

The Pharmaceutical Information Program is a major step forward in enhancing patient safety. The program will help prescribers select the best medication to avoid drug interactions and duplications of therapy, including prescription drug abuse. PIP will also help health professionals sort through the numerous medications a person may be taking when treating medical conditions, or where several prescribers are involved in a patient's care.

PIP is part of a wider government strategy to create an electronic health record.