Patient Confidentiality and the Collection, Use and Disclosure of Personal Health Information

Disclaimer

SCPP provides general guidance on privacy matters. If you require more information, we encourage you to speak with your Privacy Officer, to refer to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) website, and/or to seek advice from your legal counsel. **Further, it is advisable to always check directly with the applicable legislation before collecting, using or disclosing personal health information to ensure compliance.**

DEFINITIONS

In this document,

"**Pharmacy Professional**" means licensed pharmacists, licensed pharmacy technicians and pharmacy interns (extended and student).

"**Proprietor**" means the person who controls the operation, and is the permit holder, of a proprietary pharmacy.

GLOSSARY OF ACRONYMS

HIPA - *The Health Information Protection Act.*

HIPR - *The Health Information Protection Regulations, 2023.*

PHI - personal health information

PIPEDA - the *Personal Information Protection and Electronic Documents Act.*

SCPP - Saskatchewan College of Pharmacy Professionals

1. BACKGROUND

Maintaining confidentiality is a vital part of the relationship between pharmacy professionals and their patients. All pharmacy professionals have a legal, professional and ethical obligation to protect the privacy of their patients.

In Saskatchewan, HIPA establishes the rights of individuals regarding the privacy of their PHI and the obligations of trustees with respect to the collection, storage, use, and disclosure of PHI. HIPR are HIPA's regulations that provide more details of HIPA's rules and requirements relating to PHI. See: HIPA's Founding Principles

PIPEDA is broader federal legislation that applies to private sector organizations (such as community pharmacies) and sets out the rules for how businesses must handle personal information in the course of their commercial activities (which includes PHI).

HIPA and PIPEDA both apply to community pharmacies. SCCP expects all proprietors and pharmacy professionals to be aware of and comply with their obligations under both Acts. Fortunately, the basic principles and responsibilities of HIPA and PIPEDA are very similar.

In addition to their legislative obligations, pharmacy professionals have an additional responsibility under the SCPP Code of Ethics to protect their patient's right of confidentiality.

This guidance document will focus on the rules pertaining to the collection, use and disclosure of PHI under HIPA (and HIPR - its regulations).

2. WHAT IS PERSONAL HEALTH INFORMATION (PHI)?

PHI is defined in HIPA and includes information:

1. with respect to the physical or mental health of an individual (including genetic information),
2. pertaining to any health service provided to an individual,
3. acquired in the course of providing services, and
4. gathered to register the individual (including their health services number).

HIPA applies to PHI in any form, including both paper and electronic records.

3. WHO IS REQUIRED TO PROTECT PHI?

The trustee of the PHI is ultimately responsible under HIPA to ensure that all the rules and requirements of HIPA are followed. The trustee means the person or entity that has custody and control of the records and includes any of the following:

1. the proprietor of a pharmacy,
2. a pharmacy professional employed by a non-trustee (i.e. a non-proprietor),
3. the Saskatchewan Health Authority or other public body who employs a pharmacy professional, and
4. anyone who owns or operates a privately-owned facility that delivers health services.

Everyone must follow HIPA

Whether you are the trustee, or you are employed by the trustee, or you are otherwise authorized to access PHI by the trustee**, you are nevertheless obligated to follow the rules in HIPA when collecting, using and disclosing PHI**. It is an offence for anyone to knowingly contravene HIPA and doing so could result in fines or even imprisonment.

4. COLLECTION OF PHI

PHI should be collected for the primary purpose of delivering pharmacy services to the patient. Whenever possible, PHI should be collected directly from the patient to whom it relates. Collect only the PHI that is needed for the purpose. Once in the pharmacy's possession, the trustee is responsible to ensure that PHI is accurate, complete and safeguarded. Further, the trustee **must provide access to the records upon request from the patient.**

Unauthorized collection occurs when PHI is collected, acquired or received for purposes that are not authorized by HIPA. Anyone that inadvertently receives or acquires PHI (who does not "need-to-know" that information) must immediately safeguard the PHI, notify their privacy officer, contact the sender and either return or destroy the information (do not keep a copy).

5. RETENTION AND DESTRUCTION OF PHI

The duty to protect PHI includes the requirement to have appropriate procedures in place for retention and destruction of all the PHI that your pharmacy collects. For more detailed information on retention and destruction of pharmacy records see Record Retention and Destruction.

6. USE OF PHI

Once collected by the pharmacy, PHI may only be accessed or used by those who **need** that information to provide pharmacy services or need it for another legitimate purpose authorized by HIPA. This is known as the "need-to-know principle". Further, the least amount of PHI necessary for the purpose should be accessed or used. This is known as data minimization. **Both the "need-to-know" principle and data minimization should be top of mind whenever considering whether to access, use or disclose PHI.**

Unauthorized access is a privacy breach and occurs when individuals access PHI that they **do not** need-to-know, either accidentally or purposefully. Accessing PHI out of curiosity or concern is not a legitimate purpose.

In addition to using PHI to provide pharmacy services, PHI may also be used for the purposes listed in sections 27, 28 and 29 of HIPA (the sections related to disclosure of PHI). Other legitimate purposes could include to assess the need for further services, to comply with a court order, to obtain payment for the provision of pharmacy services, to prepare for a legal proceeding, etc. (see section below on disclosure of PHI).

Much of the PHI that is accessed and used by pharmacy professionals is done through PIP (The Pharmaceutical Information Program) and eHR Viewer (The electronic Health Record). For more on this topic and specific guidance on accessing PHI through PIP and eHR Viewer see: Accessing PIP and eHR Viewer

Consider these questions every time PHI is accessed in your pharmacy:

Who needs to know the information? **Only the individuals involved in providing the pharmacy services to the patient.**

Why do they need to know it? **The PHI is required to support or provide pharmacy services.**

What do they need to know? **Only the minimum amount of information required to provide the services.**

7.DISCLOSURE OF PHI

Disclosure means sharing information outside your organization. PHI can **only be disclosed with the consent of the patient** unless the disclosure is otherwise authorized by HIPA. The need-to-know principle (disclosing PHI only to those who have a need to know it) and data minimization (disclosing the least amount of PHI necessary for the particular purpose) must also be applied anytime PHI is disclosed.

7.1 De-identify Information

HIPA does not apply to de-identified PHI. “De-identified personal health information” is PHI from which any information that may reasonably be expected to identify an individual has been removed. Whenever possible, PHI should be de-identified before it is disclosed. Information has been adequately de-identified if it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual. [HIPA s. 2 (1)(d) and 3(2)(a)].

7.2 Disclosure with Consent

When PHI cannot be de-identified, consent is generally required to disclose it.

Unless they tell you otherwise, patients are **deemed** to consent (meaning consent is presumed and it is not necessary to obtain explicit consent) to the disclosure of their PHI when it is being shared:

1. for the purpose of providing or supporting pharmacy services;
2. for the purpose of arranging, assessing the need for, providing, continuing or supporting the provision of, a service requested or required by the patient, and
3. with their next of kin or someone with whom they have a close relationship, but **only** if it **relates to pharmacy services they are currently receiving** and only **if the patient has not asked you not to share their PHI.** Discretion should be used taking into account the sensitivity of the PHI. When in doubt, get the patient's consent before sharing information with their family or friends.

   [HIPA s. 27(2)]

In all other situations where consent is required, **seek informed consent directly from the patient before disclosing PHI** (unless the patient lacks the capacity to consent in which case consent must be obtained from their substitute decision maker. For guidance on substitute decision making see: Health Care Directives, Substitute Decision Making and Powers of Attorney). Informed consent in these circumstances means the patient is advised and understands the nature of the PHI that will be disclosed, why the PHI is being disclosed, who the PHI will be disclosed to and the likely consequences of disclosing or not disclosing the PHI (if any). Remember that consent is situation specific and is required each time a new disclosure is being contemplated.

7.3 Disclosure without Consent

There are a limited number of situations where disclosure of PHI without consent is permitted either under HIPA, or another statute or legal document. Never disclose PHI unless the authority for the disclosure has been clearly identified. If disclosure is in response to a request, ask the person requesting the PHI to cite the authority for the disclosure.

HIPA's disclosure without consent provisions are not requirements

Unless the situation is one in which PHI must be disclosed to a third party (eg. receipt of a subpoena, suspected child abuse), trustees are not required to disclose PHI, even though HIPA may permit them to do so. Discretion should be used to determine whether disclosure is in the best interest of the patient or in the public interest.

Some examples of circumstances when PHI **may** be disclosed without the patient's consent include:

1. Disclosure to other pharmacy professionals and/ or other health care professionals for bona fide medical reasons where, the information is necessary in the interests of the patient to protect the mental or physical health or safety of the patient.
2. Disclosure to the person who is authorized under *The Health Care Directives and Substitute Health Care Decision Makers Act, 2015* to make a health care decision on behalf of a patient who is not competent to make the decision. The PHI **must be limited to the information needed** to make the particular health care decision. See Substitute Decision Makers, Health Care Directives and Powers of Attorney.
3. Disclosure is necessary to comply with the law. For example, a warrant, subpoena or court order compelling the release of PHI, an inspector authorized under the *Controlled Drugs and Substances Act* or the *Food and Drugs Act* makes a request to access records pertaining to Narcotic and Controlled Drugs, Benzodiazepines and other Targeted Substances, or an SCPP investigator requires records for the purpose of an investigation.
4. Police request the PHI for the purpose of an investigation under the *Criminal Code* or the *Controlled Drugs and Substances Act*. See Disclosure of Personal Health Information to Police**.**
5. Disclosure of PHI is required to by the pharmacy's legal counsel for use in providing legal services to the pharmacy.
6. Disclosure is necessary for monitoring, preventing or revealing fraudulent, abusive or dangerous use of publicly funded health services.
7. Disclosure to Information Management Service Providers for the purpose of storing, managing, archiving, destroying PHI or for other information technology services, where an appropriate written agreement with the service provider is in place.

The above list is not exhaustive. For more information on disclosure without consent, refer to the following supplemental guidelines:

Use and Disclosure of Personal Health Information for Secondary Purposes

Disclosure of Personal Health Information to Police

Disclosure of the Personal Health Information of Minors to Parents/Legal Custodians

Substitute Decision Makers, Health Care Directives and Powers of Attorney

7.4 Document the Disclosure

Every time PHI is disclosed, the following should be documented:

1. The name of the person requesting the PHI and confirmation of their identity (if the disclosure is in response to a request);
2. The nature of the request and the reason the PHI is required;
3. Whether consent was obtained from the patient, or the reasons for not seeking consent;
4. Whether consent was given or refused;
5. The authority for the disclosure (eg. the HIPA provision or the court order, etc.); and
6. A description of the PHI that was disclosed.