



Pharmacist's Personal Information Privacy Code

Executive Summary

Overarching Principle

The principles set out in this Code reflect the need to protect the privacy of personal information, and to obtain an individual's consent to the collection, use and disclosure of such information, unless collection, use or disclosure is permitted in accordance with the law.

Individual Rights and Responsibilities

1. **PRIVACY** — Individuals have a right of privacy with respect to their personal information.
2. **CONSENT** — Individuals have the right to provide or withhold consent with respect to the collection, use, disclosure, or access of their personal information.
3. **KNOWLEDGE** — Individuals have a right to know what is happening with their personal information.
4. **INDIVIDUAL ACCESS** — Individuals have the right to access their own personal information.
5. **ACCURACY** — Individuals have the right to have their personal information recorded as accurately as possible and to review and amend their health records to ensure accuracy.
6. **REMEDY** — Individuals have the right to an independent remedy when they suspect a breach in the privacy of their personal information.

Provider and Organization Obligations

1. **CONFIDENTIALITY** — Providers and organizations have an obligation to treat personal information as confidential.
2. **TRUSTESHIP AND ACCOUNTABILITY** — Providers and organizations entrusted with personal information have an obligation to safeguard the privacy of individuals and the confidentiality of this information.



3. **COLLECTION AND USE — PERSONAL INFORMATION**

- a) Providers and health care organizations require identifying information to provide direct care to individuals.
- b) Except in exceptional circumstances, identifying information must only be used with the consent of the individual. Circumstances where consent may be inappropriate or not required include:
 - ▶ emergency situations
 - ▶ in response to a court decision or order
 - ▶ in accordance with legislation
- c) Identifying information may also be reasonably collected, disclosed or used for purposes other than, but closely connected to, the provision of diagnosis and treatment or care of patients, providing the individual about whom the data is collected has been informed of these potential uses and has given consent. In addition, collection and use of personal information should be kept to a minimum.

4. **ACCESS AND USE — DE-IDENTIFIED HEALTH INFORMATION**

- a) Access to and use of de-identified information should be available to improve population health status and for approved research.

5. **SECURITY** — Security safeguards must be in place to protect the integrity and confidentiality of health information.

6. **IMPLEMENTATION AND COMPLIANCE**

- a) Providers and organizations should implement policies, procedures and practices to achieve privacy protection.
- b) Providers and organizations should also make specific information regarding their policies and practices relating to the management of personal information readily available to individuals.
- c) Organizations should put procedures in place to receive and respond to complaints or inquiries about their policies and procedures.



Background

The Canadian Pharmacists Association (CPhA) is the national association providing leadership for pharmacists in all areas of pharmacy practice. CPhA strongly believes that Canadians' right to privacy protection is fundamental. As pharmacists, we strongly support privacy protection as attested by the fact that we remain one of the most trusted professions. Pharmacists have managed confidentiality issues with a high degree of professionalism over the years and are committed to ensuring that the privacy of their patients is safeguarded. Therapy with prescribed medications is a collaborative process involving the patient, the physician, the pharmacist, and other health care providers. Pharmacists have a unique knowledge about drugs and their proper use that can be used to enhance the care of patients on an everyday basis. The provision of pharmaceutical care improves patient health and well-being. Pharmaceutical care requires that a professional relationship between the patient and the pharmacist be established and maintained, that records are kept of medications provided to a patient, and that patient-specific medical information be evaluated to develop a care plan. All of these steps in the pharmaceutical care process require the collection, review and sharing of personal information.

Due to its sensitive and personal nature, health information merits special protection by health care providers and legislators. Health information includes intimate details about an individual's physical, emotional and/or mental health and is most commonly confided to health care providers and others who provide services with the explicit or implicit understanding that such information will be kept confidential. Most often, this personal information is shared with health care providers with the expectation that they will provide cure or relief and prevent harm.

Because of its nature, there is the expectation that health information will be used for the informed benefit of the individual who puts his/her trust in a health care provider or health care facility. Therefore, higher levels of privacy protection must be afforded to health information than to other forms of personal information. This circumstance necessitates the development, adoption and implementation of specific principles for health information privacy protection that encompass the rights and responsibilities of individuals as well as legitimate societal concerns and obligations of the health system.

In addition to information concerning the treatment of their patients, pharmacists will also possess other forms of their personal information. This could include information concerning their employment or spousal relationships, credit card and insurance information. This information should be treated in the same manner as information concerning patient treatment.

The Pharmacist's Personal Information Privacy Code ("Code") articulates principles for protecting the privacy of patients, the confidentiality and security of their personal information and the trust and integrity inherent in the therapeutic relationship between pharmacists and patients.

The purpose of this Code is not to set out the specific policies and procedures which will be followed by pharmacists in the course of their business. Rather, it is intended to set out broad principles, providing the basis for individual pharmacists to establish their own policies and procedures. Further, pharmacists are also required to comply with applicable provincial and/or federal legislation.



Section A — Scope

The Pharmacist's Personal Information Privacy Code has been produced by pharmacists to protect the privacy of their patients, the confidentiality and security of their health information, and the trust and integrity inherent in the therapeutic relationship. The Code follows the ten standards established by the *Canadian Standards Association's Model Code for the Protection of Personal Information* ("CSA Code"). The CSA Code is a central part of the federal *Protection of Personal Information and Electronic Documents Act* (PIPEDA). Also, the Code is based on the *Principles for the Privacy of Protection of Personal Health Information in Canada* (2000) developed by the Privacy Working Group.¹ The Code and the accompanying guidelines provide instruction and guidance with respect to health information collection, use, disclosure and access and they have been structured in such a way as to take into account the particular challenges involved in the implementation steps needed to maintain privacy and confidentiality of personal information in pharmacy practice.

- ▶ This Code has been developed by pharmacists in their capacity as clinicians and in recognition of their principal obligation to patients.
- ▶ This Code recognizes the potential benefits of the use of health information for secondary purposes, including teaching, research and system planning, and contains provisions to permit such use.
- ▶ The principles that make up this Code are interrelated. Pharmacists adopting this Code should adhere to these principles as a whole.
- ▶ Pharmacists should strive to incorporate compliance with this Code into their everyday practice; however, they may tailor this Code by modifying or adding principles provided the changes afford no less protection to the privacy of patients and the confidentiality and security of their health information.
- ▶ Statements containing "must" indicate requirements that must be met by any pharmacist who wishes to adopt this Code and be recognized for having done so. The use of "should" indicates a recommendation or aspiration.

Section B — Principles

Overarching Principle

The principles set out in this Code reflect the need to protect the privacy of personal information, and to obtain an individual's consent to the collection, use and disclosure of such information, unless collection, use or disclosure is permitted in accordance with the law.

¹ CPhA acted as the secretariat for a national privacy working group of health organizations. This group was composed of representatives from the Canadian Dental Association, the Canadian Medical Association, the Canadian Pharmacists Association, the Canadian Health Care Association, the Canadian Nurses Association and the Consumer Association of Canada. The work of the group was funded by the Knowledge and Policy Development Division of Health Canada.



Individual Rights and Responsibilities

The principles in this section are followed by a short description with the objective of bringing precision to the application of the principle.

1. **PRIVACY** — Individuals have a right of privacy with respect to their personal information.

Individuals have the right to determine to whom, when, how, and to what extent they will disclose their personal information and to exercise control over use, disclosure, and access concerning identifying information collected about them. Individuals also have a right to know how their personal information is to be used and safeguarded. Individuals must be informed of their privacy rights.

2. **CONSENT** — Individuals have the right to provide or withhold consent with respect to the collection, use, disclosure, or access of their personal information.

Except as permitted by legislation, consent must be obtained, orally or in writing, whenever a person's personal information is collected, used, or disclosed. Consent need not always be expressly given through written or oral methods but may in certain circumstances be given orally, or may be implied depending on the context. The circumstances under which collection, use and disclosure of personal information is permitted in the absence of express consent are prescribed in applicable provincial and federal legislation.

3. **KNOWLEDGE** — Individuals have a right to know what is happening with their personal information.

Patients must either have or be provided, by reasonable means, with information about what will happen with their personal information. This must include information about the purpose for the collection, use or disclosure, and by whom, when, how, and to what extent their personal information is being or will be collected, disclosed, stored, accessed, and used.

4. **INDIVIDUAL ACCESS** — Individuals have the right to access their own personal information.

Individuals must be provided with access to their identifying information in a timely fashion, at minimal or no cost, and with professional interpretation, as needed.

5. **ACCURACY** — Individuals have the right to have their personal information recorded as accurately as possible and to review and amend their health records to ensure accuracy.

Individuals who have reviewed their information and believe it to be inaccurately recorded or false have the right to require amendments and to have their amendments appended to the health information. Individuals have a responsibility to ensure that the personal information they disclose is accurate.

6. **REMEDY** — Individuals have the right to an independent remedy when they suspect a breach in the privacy of their personal information.

Individuals must have a clear and open process to address concerns about a suspected breach of their privacy. Individuals must be informed of the outcome of the process. In the event of a disagreement, a dispute resolution process must be initiated, involving a neutral third-party mediator. Failing such a process, individuals must be informed of their right to have their complaint investigated by the appropriate federal or provincial Privacy Commissioner.



Provider and Organization Obligations

The principles in this section are followed by a short description with the objective of bringing precision to the application of the principle.

1. **CONFIDENTIALITY** — Providers and organizations have an obligation to treat personal information as confidential.

Personal information, including identifying information, must not be disclosed or made accessible to others unless authorized by express consent, or where legislation provides for such disclosure in the absence of consent; for example, where disclosure is made to a person, such as a health care provider who needs the information because of an emergency that threatens the life, health or security of an individual, or pursuant to a Court order.

Disclosure of personal information is also permitted in the absence of consent for statistical or scholarly study or research purposes that cannot be achieved without disclosing the information, when it is impracticable to obtain consent, and the organization informs the Commissioner of the disclosure before the information is disclosed.

Consent to exchange information between health care providers and organizations to provide individual care or prevent harm may be implied as long as the disclosure is one to which the individual would reasonably be expected to agree.

2. **TRUSTEESHIP AND ACCOUNTABILITY** — Providers and organizations entrusted with personal information have an obligation to safeguard the privacy of individuals and the confidentiality of this information.

Health care providers, organizations and government agencies are accountable for safeguarding and maintaining the privacy and accuracy of personal information. They are first and foremost accountable to the individuals whose health information they possess. There is also a mutual responsibility among trustee organizations and providers to uphold privacy protection rules and processes. Health information trustees include, but are not limited to, professional colleges, private companies, health facilities and agencies, regional boards, governments, corporations and health care providers.

3. **COLLECTION AND USE — PERSONAL INFORMATION**

- a) Providers and health care organizations require identifying information to provide direct care to individuals.

Disclosure, collection and use of identifying information is required for the provision of appropriate diagnosis, treatment and care of an individual. This includes disclosure of:

- ▶ accurate personal information by an individual to a care provider
- ▶ identifying information between those providing care to the individual

- b) Except in exceptional circumstances, identifying information must only be used with the consent of the individual. Circumstances where consent may be inappropriate or not required include:

- ▶ emergency situations
- ▶ in response to a court decision or order
- ▶ in accordance with legislation



- c) Identifying information may also be reasonably collected, disclosed or used for purposes other than, but closely connected to, the provision of diagnosis and treatment or care of patients, providing the individual about whom the data is collected has been informed of these potential uses and has given consent. In addition, collection and use of personal information should be kept to a minimum.

When using or disclosing identifying information or when requesting health information from another provider or organization, the provider or organization must make reasonable efforts to limit such collection, use or disclosure to the “minimum necessary” to accomplish the intended purpose, use, disclosure or request.

The following are examples of disclosures for purposes related to the provision of diagnosis or treatment:

- ▶ Quality assurance and system effectiveness: disclosure of “minimum necessary” identifying information to organizations and agencies authorized by legislation to collect such information by individuals, providers, facilities, organizations and governments may be required to assure quality care and promote effectiveness and efficiency in the health care system and its many components.
- ▶ The disclosure, collection, and use of the “minimum necessary” identifying information for billing or payment purposes. Disclosure of limited or “minimum necessary” identifying information to payers by individuals, providers or other payers is required to ensure payment from third parties, e.g., governments, insurance companies, employers.

4. ACCESS AND USE — DE-IDENTIFIED HEALTH INFORMATION

- a) Access to and use of de-identified information should be available to improve population health status and for approved research.

Health care providers, organizations, universities, scientific bodies, governments and other agencies are accountable for protecting, maintaining, and improving population health through research.

An example of when de-identified health information may be used includes:

- ▶ Research: disclosure of de-identified information to individuals, organizations and agencies, authorized by an established research ethics board, by individuals, providers, facilities, organizations and governments may be required for biomedical research, applied clinical research, population health research, health systems research and market research.

5. SECURITY — Security safeguards must be in place to protect the integrity and confidentiality of health information.

Health care providers, organizations and government agencies must have in place policies and procedures to ensure the security of the data collected and used. These policies and the remedy available must be publicly known.

Personal information must be retained only as long as is necessary for the fulfilment of the purposes for which it was collected.

Information trustees must establish a written policy concerning the retention and destruction of personal information and must comply with that policy.



6. IMPLEMENTATION AND COMPLIANCE

- a) Providers and organizations should implement policies, procedures and practices to achieve privacy protection.

These policies, procedures and practices should be clearly delineated and known by all involved. Failure to protect privacy and confidentiality should result in sanctions imposed by professional organizations and institutions as well as those defined under federal, provincial and territorial law. These policies should be open and transparent.

- b) Providers and organizations should also make specific information regarding their policies and practices relating to the management of personal information readily available to individuals.

- c) Organizations should put procedures in place to receive and respond to complaints or inquiries about their policies and procedures.

Section C — Health Information Policies

Personal information trustees must have in place and implement policies, procedures and practices that give effect to the principles of this Code. The trustee's policies must be readily available to patients and should include information about practices and procedures. The following list illustrates the content that should be included in an information policy for a pharmacy, institution or other health information trustee.

Personal information policies, procedures and practices should be tailored to the specific health care setting of the trustee and must address and provide for:

- ▶ Complying with and giving effect to the principles of this Code.
- ▶ Protecting the security of health information.
- ▶ Ensuring the accurate recording and integrity of health information.
- ▶ Documentation of all purposes for which the personal information trustee uses or discloses the personal information it collects, including to whom it permits access to what information, in what format and whether consent is required.
- ▶ Documentation of what personal information may be linked to other pieces of information.
- ▶ Documentation of what personal information is made available to third parties.
- ▶ Allowing access only to authorized users in the appropriate format and for the limited purposes for which they are authorized.
- ▶ Tracking and recording all access to personal information (audit trail).
- ▶ Identification of the person who is accountable for the policies, procedures and practices and to whom complaints or inquiries can be made.



- ▶ Receiving and responding to complaints and inquiries.
- ▶ Ensuring that persons who collect, use, disclose or access personal information can be held accountable and are under an enforceable duty to keep information secure.
- ▶ Ensuring that persons who work for or in the health institution or pharmacy know and receive sufficient training about this Code and related institutional policies, procedures and practices to ensure accountability.
- ▶ The means of gaining access to one's own personal information held by the health institution.
- ▶ Making available information that a particular patient specifically requests or reasonably can be presumed to wish to know.
- ▶ Ensuring that patients have, or by reasonable means are provided with, knowledge about their personal information and that consent is sought and obtained as appropriate.
- ▶ Specification of minimum and maximum retention periods and rules for the succession, transfer and destruction of personal information.

Appendix A — Glossary

The following definitions apply in this Code:

Accountability means having clearly defined and understood responsibilities in connection with personal information, agreeing to accept those responsibilities, and being subject to appropriate sanctions for failing to fulfil accepted responsibilities.

Authorized means collection use or disclosure of or access to personal information which occurs with patient consent or within the provisions of this Code.

Authorized user is someone permitted to collect, use, disclose or access personal information under the provisions of this Code, who is properly instructed on his/her limits and responsibilities and can be held accountable for his/her compliance.

Collection means the act of accessing, receiving, compiling, gathering, acquiring or obtaining personal information from any source, including third parties, and by any means. It includes information collected from the patient as well as secondary collection of this information in whole or in part by another provider or user.

Confidentiality means that personal information that is confided by a patient is to be kept secret and not disclosed or made accessible to others unless authorized by patient consent. A breach of confidentiality occurs whenever a health professional discloses or makes personal information available to others without, or inconsistent, with the patient's consent.

Consent must be voluntary, informed consent. Consent is a concurrence of will and knowledge. Informed consent may be either "express" or "implied".

Express consent is given in writing or verbally, is unequivocal and does not require any inference on the part of the person or organization seeking consent.

Implied consent is not given by a patient in writing or verbally but understood from the circumstances surrounding the procedure or treatment at issue or could be reasonably assumed from the past or current actions of the patient.



De-identified Health Information is information from which any information that may reasonably be expected to identify an individual has been removed.

Disclosure means the provision of personal information to a third party for any reason, or making personal information available for a third party to collect. It includes any transfer or migration of personal information from one provider or user to another.

Emergency Situations mean those instances when health care must be provided to preserve life or prevent severe harm to a patient who is unable, owing to the circumstances, to be cognizant of the context and whose surrogate is not immediately available to make decisions on the patient's behalf.

Knowledge means the patient's awareness of what can, will, or must happen with the health information he/she confides or permits to be collected.

Patient means the person about whom personal information is collected and, for the purposes of this Code, may also mean a surrogate or guardian acting on behalf of this person.

Personal Information is information about an identifiable individual, excluding the name, title, business address or telephone number of an employee of an organization. This includes any information about a patient that is confided or collected in the therapeutic context, including information created or generated from this information. It includes all information formats.

Identifying Information means information that identifies an individual or for which there is a reasonable basis to believe that it could be utilized, either alone or with other information, to identify an individual.

Pharmacist means a person who is registered and entitled under the laws of a province or territory to practise pharmacy in that province or territory.

Purpose means an end or aim for which personal information is collected, used, disclosed or accessed.

Provider means a health professional, institution or pharmacy that delivers health care services or products in the therapeutic context.

Right of Privacy includes a patient's right to determine with whom he/she will share information and to know of and exercise control over use, disclosure and access concerning any information collected about him/her; it entails the right of consent.

Security means reasonable precautions, including physical and technical protocols, to protect personal information from unauthorized collection, use, disclosure and access, and to ensure that the integrity of the information is properly safeguarded. A breach of security occurs whenever personal information is collected, used, disclosed or accessed other than as authorized, or its integrity compromised.

Trustee means health care provider, health care facility, health service agency, or public bodies such as federal/provincial/territorial government departments and agencies that have either a duty to protect the privacy of individuals in the collection, use, disclosure, security, retention and destruction of their personal information or a duty to assist individuals in gaining access to their own personal information.

Use of Information means the sharing, employment, application, utilization, examination, or analysis of such information by a health care provider, organization, agency, or body that maintains such information.