

COMPENDIUM

PERSONAL HEALTH INFORMATION PRIVACY ACT, 2000

An Act respecting Personal Health Information and related matters

BACKGROUND

Currently, in Ontario there is no legal protection for personal health information held in many settings, and rules about who may use the information and how are few and inconsistent. Many jurisdictions have enacted or are developing legislation to protect the privacy, confidentiality and security of health information.

In October 2000, a consultation paper entitled Ontario's Proposed Personal Health Information Privacy Legislation for the Health Sector (Health Sector Privacy Rules) was released for public consultation. The consultation paper was widely distributed to about 5,000 organizations and individuals across the province, inviting written submissions. Roundtable meetings were held in a number of locations across Ontario. Over 100 written submissions were received.

This consultation built on earlier consultation processes. In June 1996 a consultation paper, A Legal Framework for Health Information, was followed by regional roundtable meetings and resulted in over 100 written submissions. In November 1997, the Draft Personal Health Information Protection Act, 1997 was released for public consultation. The Draft Act and a plain language overview were sent for review and comment to 1,000 individuals and organizations, and the overview alone to a further 4,000. Regional consultation meetings were held across the province and approximately 200 written submissions were received.

The advice received over the course of these three rounds of consultation was used to revise the draft legislation and is reflected in this Act.

The Personal Health Information Privacy Act, 2000 provides consistent and comprehensive rules that are currently lacking for many individuals and organizations that collect personal health information. The goals of the legislation are to protect the privacy, confidentiality and security of personal health information, and to facilitate the use of personal health information to improve quality of care for patients and effective use of health care resources.

FEATURES OF THE ACT

I. Purposes, Definitions and Interpretation

The Act provides rules for the collecting, using, storing, disclosing and disposing of personal health information. It requires that personal health information be kept confidential and secure. It gives people a right to see their own personal health information and to request corrections. It sets out who can act on another person's behalf with respect to personal health information and in what circumstances. It also establishes remedies for violations of the Act.

The Act applies to "health information custodians". These are listed individuals or organizations that have custody or control of personal health information because of the work that they do or in connection with the powers or duties they perform. Examples of custodians are: health care professionals, hospitals, health clinics, nursing homes, the Minister of Health and Long-Term Care, and some other government programs.

"Personal health information" is defined as information about an identifiable individual who is living or deceased, whether or not the information is recorded, that relates to his or her physical or mental health or well-being, provision of health care, donation of a body part or bodily substance, payments or eligibility for health care, health number, or registration information. Registration information refers to information relating to an individual collected or created for registering the individual in connection with a custodian's services or benefits such as name, address, telephone number, date of birth, and signature, but does not include information about the individual's health status or health care. Personal health information also includes information about a health care provider or substitute decision maker where linked to information about an individual's health or health care.

II. Application of the Act

The Act sets out the specific circumstances where it does not apply. For example, it does not apply to recorded personal health information that is more than 100 years old, information relating to labour relations affecting the individual or the employment of the individual, the child abuse register, the adoption disclosure register, and anonymous or statistical information where an individual cannot be identified.

Subject to few exceptions, if there is a conflict between a confidentiality provision in this Act and one in another Act, this Act prevails unless this Act or the other Act provides otherwise.

III. General Limitations

Personal health information must not be collected, used or disclosed if other information can serve the purpose. The collection, use, or disclosure must be limited to registration information if registration information serves the purpose. If personal health information is needed, no more information than is reasonably necessary to meet the purpose can be collected, used or disclosed. To the extent reasonably possible, personal health information must be

collected, used or disclosed in a way that conceals the identity or keeps identifiers of the individual separate from the information.

A health information custodian must also comply with any standards set out in the regulations and any requirements concerning registration information or the electronic transfer of personal health information set out in the regulations, where applicable.

If a health information custodian that is also an institution under the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act* wishes to perform computer matching involving two or more databases, and if the results will be used to directly affect an individual, some special safeguards apply, including review of certain information by the Information and Privacy Commissioner.

The Act sets out the responsibilities of employees and other people who work on behalf of a custodian, including an agent, a solicitor, a student, or a volunteer. The Act also sets out the role and responsibilities of an "information manager" who, on behalf of a custodian, processes, stores or disposes of records that contain personal health information or provides information management or information technology services to the custodian with respect to records that contain personal health information. A written agreement is required between the information manager and the custodian setting out responsibilities, safeguards and notification requirements.

IV. Practices to Protect Personal Health Information

The Act sets out that a health information custodian must have administrative, technical and physical safeguards and practices to protect the integrity, accuracy, confidentiality and security of personal health information in the custodian's custody or under its control.

A health information custodian must have a written policy regarding the retention and disposal of records containing personal health information.

A health information custodian must have in place a contact person among the custodian's staff to help the organization comply with the legislation, to respond to inquiries about information practices, and to receive complaints from the public.

In addition, custodians are to be required to set out their information management practices in writing, and to make this information available to the public. The information is to include information about a contact person, and procedures for access and for complaints.

V. Consent Concerning Personal Health Information

Where a person's consent is required under this Act or any other Act for collecting, using or disclosing personal health information, it must be an informed consent. An informed consent includes information that a

reasonable person would require in the circumstances to make a decision about the collection, use or disclosure of personal health information. This could include the identity of the person who will be collecting, using, disclosing or receiving the information, the purpose of the collection, use or disclosure, how much information is to be collected, used or disclosed, and the reasonably foreseeable consequences of giving or withholding consent.

A consent may be time-limited and may be revoked by the individual who gave it at any time. A health information custodian who receives a consent to a collection, use or disclosure of personal health information about an individual that the individual gives is entitled to assume that the consent fulfills the requirements set out in the Act unless it is not reasonable to assume so.

VI. Collection, Use and Disclosure of Personal Health Information

A health information custodian cannot collect personal health information unless the collection is expressly authorized by or under an Act or necessary for a lawful purpose related to a function or activity of the custodian.

As a general rule, a custodian must collect personal health information about an individual directly from that individual and inform that individual of the purpose for collecting the information unless it is reasonable to infer the purpose in the circumstances.

There are some circumstances set out in the Act where information can be collected from someone else. For example, where the individual consents to another manner of collection, another Act permits another manner of collection, or collection of the information directly from the individual is not reasonably practicable.

A custodian has a duty of confidentiality and is required to maintain the confidentiality of the personal health information in the custodian's custody or control and to use or disclose it only as permitted or required under this Act and in accordance with the custodian's lawful purposes.

A health information custodian may use personal health information for limited purposes set out in the Act. These include, for example, the purpose for which the information was collected or created, a directly related purpose, a purpose to which the individual consents, a purpose for which the information may be disclosed to a custodian under this Act, planning or delivering programs of a custodian, and detecting or preventing fraud.

Before using or disclosing personal health information, a health information custodian must take steps that are reasonable in the circumstances to ensure that the information is accurate, complete and not misleading.

A person who receives personal health information from a custodian cannot use or disclose that information for any purpose other than the purpose for which the custodian was authorized to disclose it, a directly related purpose,

or a purpose for which the individual consents, or where authorized by some other law.

A health information custodian must provide an individual with information about expected and unanticipated uses and disclosures as prescribed in the regulations.

A custodian cannot use or disclose an individual's personal health information to market services or for market research without the individual's consent.

A custodian that is a facility or organization that provides health care may use or disclose an individual's name and address for fundraising activities for charitable or philanthropic purposes related to the custodian's operations as long as the individual has not requested that the custodian not use or disclose the information for these purposes. Individuals would be notified that they have a right to opt out.

Guidance is also to be provided in regulations regarding conditions for fundraising and any prohibitions.

As a general rule, a custodian may disclose personal health information about an individual only if that individual consents.

However, the Act builds on existing laws that allow disclosure of personal health information without consent under limited exceptions. These exceptions are set out in the Act. They include disclosure to a custodian who is a health care practitioner or facility/organization that provides health care for the purpose of providing or assisting in providing health care to the individual; for the purpose of determining or verifying eligibility of an individual to receive health care or other benefits; for the purpose of managing the custodian's programs or services; for the purpose of carrying out an inspection or investigation; or to eliminate or reduce a significant risk to an individual's safety.

As a custodian, the Minister of Health is subject to the same rules as the other custodians under the Act. However, in order to fulfil the responsibilities of managing the health system, planning for the system's future needs, evaluating its effectiveness, detecting and preventing fraud, verifying information held by the Ministry and administering or enforcing Ministry legislation, the Act allows custodians to disclose personal health information to the Ministry for these purposes. In some circumstances, the Minister may require certain custodians to disclose personal health information to it for these purposes. If the program or service is health-related but not funded in whole or in part by the Ministry, the Information and Privacy Commissioner must be given an opportunity to review and comment before such a requirement to disclose. Both the Minister and the Commissioner must consider the public interest served and the privacy interests of the individual before such disclosure is required.

The Minister may direct that information be disclosed to another organization designated in the regulations for the above-stated purposes. This organization must enter into an agreement with the Minister that sets out terms including that the information may be used or disclosed only for the purposes set out in

the agreement, and that the organization must comply with safeguards respecting the confidentiality and security of the information.

Personal health information may be disclosed to a researcher for the purpose of a research project or program if certain conditions are met. Generally, a health information custodian may disclose personal health information that has previously been recorded to a researcher for the purpose of a research project or program if the researcher has obtained the approval of a research ethics review body designated by the regulations. The research ethics review body determines, among other things, whether the consent of individuals must be obtained before use or disclosure for the research.

Personal health information can be disclosed under certain circumstances in a proceeding. However, health care practitioners and facilities or organizations that provide health care must not disclose personal health information about their patients or clients in proceedings unless they have consent or the court or other body holding the proceeding determines that the disclosure is essential in the interests of justice.

Where a statement is provided by a physician, psychologist or other appropriate health care provider that disclosure of the record will likely result in harm to the treatment of the individual, injury to the mental condition of, or bodily harm to, another individual, the custodian shall not disclose the record unless ordered to do so by the court or other body holding the proceeding. This order cannot be made until a hearing that excludes the public has been held to determine whether or not the information should be disclosed. This does not apply in certain proceedings, for example, a proceeding in which the individual relies on his or her physical or mental health as an element of the claim or response in the proceeding. It would also not apply to a proceeding where the competency, conduct, actions, licensing or registration of a person is in issue.

Personal health information can be disclosed without consent if permitted or required under an Act of Ontario or Canada. This continues to allow, for example, reporting of suspected child abuse under the *Child and Family Services Act*, and reporting of required information to the Workplace Safety and Insurance Board under the *Workplace Safety and Insurance Act, 1997*.

The Act includes rules on use and disclosure of personal health information by custodians outside Ontario. A health information custodian that has collected personal health information in Ontario cannot use or disclose the information outside Ontario unless the use or disclosure would be permitted in Ontario by this Act and appropriate steps are taken to preserve the confidentiality of the information.

VII. Quality of Care Information

The Act has provisions dealing with information collected or prepared exclusively for a certain kind of committee in a hospital, or other entity prescribed by the regulations (e.g. health care provider peer reviews, error and risk management, hospital quality assurance, ethics review). The Act

protects such information from being used in a proceeding. As well, witnesses in proceedings cannot be required to testify about or give out such information. This approach reflects the public interest in promoting thorough reviews of patient care. Quality of care information does not include originals or copies of hospital or facility records that were not prepared exclusively for this kind of committee.

VIII. Access to Records of Personal Health Information

With very few exceptions, an individual has a right to see his or her record of personal health information. The Act sets out the process for obtaining access to one's record pursuant to a written request by the individual or, in certain circumstances, a substitute decision maker.

Note that nothing in this Part is intended to restrict the normal communication between a health information custodian and an individual with respect to personal health information about the individual that is in the custody or under the control of the custodian.

A parent of a child who is less than 16 years of age is entitled to have access to a record of personal health information about his or her child unless the record relates to treatment within the meaning of the *Health Care Consent Act, 1996* about which the child has made a decision on his or her own, or counselling in which the child has participated on his or her own under the *Child and Family Services Act*.

The Act sets out the limited circumstances under which a custodian may refuse to give an individual access to all or part of his or her personal health information, for example, where the access could reasonably be expected to result in harm to the individual's treatment or recovery or injury to the mental condition of, or bodily harm to, another individual, or the access could reasonably be expected to constitute an unjustified invasion of another individual's personal privacy.

If a health information custodian refuses an access request in whole or in part, the individual is entitled to make a complaint to the Information and Privacy Commissioner.

An individual may request that a custodian amend his or her personal health information where he or she believes there has been an error or omission. The custodian has a duty to either amend the information as requested by the individual, or attach a statement of disagreement to the record setting out the requested amendment and indicating that the custodian has not made the amendment.

IX. Substitute Decisions Concerning Personal Health Information

The Act sets out a framework for making decisions about the collection, use and disclosure of personal health information on behalf of people who are not mentally capable of making their own decisions and for people who have died.

There is a list of substitute decision makers ranked according to priority (guardian of the person or property; attorney for personal care or property; representative appointed by the Consent and Capacity Board; spouse or partner; child or parent; brother or sister; any other relative; Public Guardian and Trustee as last resort). In addition, the Act allows a capable person to authorize an individual to make information decisions on his or her behalf.

The Act defines capacity in relation to decisions about personal health information and sets out the specific people who can make a decision on behalf of an incapable individual or a deceased individual.

A substitute decision-maker must take into consideration the wishes, values and beliefs that he or she knows the individual holds (or held when capable or alive) and believes would want (or would have wanted) reflected in decisions concerning his or her personal health information.

The Act allows a person who is determined to be mentally incapable of making decisions about his or her personal health information to apply to the Consent and Capacity Board (established under the *Health Care Consent Act, 1996*) for a review of the determination. The Board also has the authority to appoint a representative to make decisions about an incapable person's personal health information on his or her behalf. An application can be made either by the incapable person or the person wishing to become the representative.

X. Information and Privacy Commissioner

The oversight body for the Act is the Information and Privacy Commissioner ("Commissioner") appointed under the *Freedom of Information and Protection of Privacy Act*. The Commissioner may delegate any of his or her powers, duties or functions under the Act to the Assistant Commissioner for Personal Health Information appointed under the *Freedom of Information and Protection of Privacy Act*.

XI. Administration and Enforcement

Any person may make a complaint to the Commissioner about any matter under the Act or the regulations made under the Act or about the information practices of a health information custodian, but not about what constitutes quality of care information. The Commissioner may require a complainant to attempt to resolve the complaint directly with the custodian or may authorize a mediator to review the complaint and try to effect a settlement.

The Commissioner may, based on information received, initiate a review if he or she has reasonable grounds to believe that a person has contravened any provision of the Act or the regulations.

The Commissioner may review a complaint in accordance with the requirements prescribed by the regulations. After a review, the Commissioner

may make comments and recommendations on the privacy protection implications relating to the complaint. If the Commissioner determines that a health information custodian has collected personal health information in contravention of the Act, the regulations or an agreement made under the Act, the Commissioner may order the custodian to cease the collection or to dispose of the records of personal health information involved.

If the complaint relates to a request for access to a record of personal health information or for an amendment of the record, the Commissioner may conduct an inquiry and may make orders to require compliance with the Act. Knowingly failing to comply with an order of the Commissioner constitutes an offence under the Act.

Other offences under the Act include: knowingly collecting, using or disclosing personal health information, including another person's health number, in contravention of this Act; knowingly obtaining or attempting to obtain personal health information when not authorized to have it; knowingly making false statements to the Commissioner; and knowingly destroying a record in an attempt to avoid giving access.

Offences under the Act can result in fines of up to \$50,000 for individuals and up to \$500,000 for corporations.

XII. Miscellaneous

The Act provides protection from liability to health information custodians and persons employed by or in the service of a custodian who act in good faith and reasonably in the circumstances. This includes people who, in accordance with the Act, do or do not collect, use, disclose, retain or destroy personal health information.

People who give or refuse consent to a collection, use or disclosure of personal health information on behalf of the individual to whom the information relates are not liable for damages for giving or refusing consent if they act reasonably in the circumstances, in good faith, and in accordance with the Act.

The Act sets out regulation powers including: fees for collecting, using or disclosing personal health information or for copying records; governing the retention and disposal of personal health information; administrative, technical and physical safeguards for managing personal health information; standards and security safeguards for information in electronic form; and other matters necessary to carry out the intent of the Act.

A committee of the Legislative Assembly must begin a review of the Act no later than three years after it comes into force and must make recommendations to the Assembly within one year of beginning the review.

XIII. Complementary Amendments

Some Acts require amendment, as their provisions are being incorporated into this Act or are no longer needed as a result of this Act. For example, the provisions of the *Mental Health Act* that deal with clinical records and of the *Long-Term Care Act* that deal with personal records are being repealed.

The *Health Cards Numbers and Control Act, 1991* is being repealed as its provisions are incorporated into this Act. This Act allows custodians to collect, use and disclose the health number under the rules of the Act but forbids or restricts its collection, use or disclosure by others.

XIV. Commencement and Short Title

The Act comes into force on a day to be named by proclamation. The short title is the Personal Health Information Privacy Act, 2000.