



Frequently Asked Questions *Personal Health Information Protection Act*

September 2015



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

This Frequently Asked Questions (FAQ) provides a general overview of the *Personal Health Information Protection Act* and *Regulation 329/04*. The information contained in this document is for general reference purposes only and should not be considered as legal advice. Legal counsel should be consulted for all purposes of interpretation. This FAQ is not binding on the Information and Privacy Commissioner of Ontario (IPC) and should not be construed to interfere with the IPC's ability to discharge its duties under the *Personal Health Information Protection Act*.

This publication is also available on the IPC website.

Cette publication est également disponible en français.

CONTENTS

Introduction	1
What is the <i>Personal Health Information Protection Act</i> and why is it necessary?	1
Overview.....	3
What is the purpose of <i>PHIPA</i> ?	3
What rights do individuals have?	3
What is the relationship between <i>PHIPA</i> and the federal <i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> ?	4
What is the relationship between <i>PHIPA</i> , the <i>Freedom of Information and Protection of Privacy Act (FIPPA)</i> and the <i>Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)</i> ?	5
Interpretation and Application of <i>PHIPA</i>	6
To whom does <i>PHIPA</i> apply?	6
What is personal health information?	6
What does “health care” mean?.....	7
What is a custodian?.....	7
Is a health care practitioner working for a non-custodian considered to be a custodian?	8
What is an agent?	9
Does <i>PHIPA</i> apply to insurance companies or employers?	10
What is an electronic service provider?	10
What is a health information network provider?	10
Who is a prescribed person?.....	11
What is a prescribed entity?	12
Practices to Protect Personal Health Information.....	13
How does <i>PHIPA</i> protect personal health information?	13
What are the notification requirements in <i>PHIPA</i> in the event of a breach?	14
Do custodians have responsibilities with respect to accountability and openness?.....	14
What are the requirements for the treatment of personal health records in the event of a change in practice?	15

Consent Concerning Personal Health Information.....	16
What are the requirements for consent?	16
What is the difference between express and implied consent?	16
When is express consent required?	17
When is implied consent sufficient?	17
What is the 'circle of care'?	18
When can custodians assume implied consent?.....	19
Are pharmacists required to obtain express consent from an individual to disclose personal health information to a third party benefits payor?.....	20
Can individuals control what personal health information is recorded in their file?	20
Can individuals withdraw their consent?.....	20
What is a 'lock-box'?	21
What are the restrictions and limitations on the lock-box?	21
What happens when an individual is incapable of providing consent?	22
Can a child under 16 years old provide consent?.....	23
Can another person, such as a family member, provide consent on an individual's behalf when picking up or dropping off a prescription?.....	23
Collection, Use and Disclosure of Personal Health Information.....	24
What are the general limitations on the collection, use and disclosure of personal health information?.....	24
Collection.....	24
What is a collection of personal health information under <i>PHIPA</i> ?	24
What are the rules regarding the collection of personal health information?	25
When can custodians indirectly collect personal health information?	25
Use.....	26
What is a use of personal health information under <i>PHIPA</i> ?	26
What are the rules regarding the use of personal health information?	26
When can personal health information be used without consent?	26

Disclosure	27
What is a disclosure of personal health information under <i>PHIPA</i> ?	27
What are the rules regarding the disclosure of personal health information?	27
When can personal health information be disclosed without consent?	28
Can personal health information be disclosed in the event of an emergency?	29
Does <i>PHIPA</i> permit disclosure of personal health information about a deceased individual?	30
Can a custodian disclose personal health information to the Workplace Safety and Insurance Board (WSIB) about an injured worker without the individual's consent?	31
Can a custodian store, access or disclose personal health information outside of Ontario?	31
Fundraising and Marketing	33
Can custodians collect, use or disclose personal health information for fundraising activities?	33
Can personal health information be collected, used or disclosed for marketing purposes?	34
Research.....	35
What are the requirements for the collection, use and disclosure of personal health information for research?	35
Are there any requirements for research ethics boards and research plans?.....	36
Ontario Health Cards and Health Numbers	37
Who can collect, use or disclose Ontario health numbers and under what circumstances?.....	37
Are other organizations permitted to request the production of a health card?.....	37
Access to Records of personal Health Information and Correction.....	39
Access	39
Are individuals permitted to access their own personal health information?	39

How do an individual obtain access to their personal health information?	40
How long does a custodian have to respond to an individual's request for access to personal health information?	40
Can a custodian refuse to provide access to an individual's personal health information?	41
Is there a fee associated with an access request?	41
What if the custodian works for a non-custodian that is covered under public sector access and privacy legislation, such as a school board or municipality?	42
Correction	42
Can individuals correct errors in their personal health information?	42
How does an individual correct errors?	43
Can a custodian refuse to correct an individual's personal health information?	43
Administration and Enforcement	44
How is <i>PHIPA</i> enforced?	44
How does an individual initiate a complaint?	44
Is there a time limit within which an individual may complain?	45
If a person is not satisfied with an IPC order, what can be done?	45
Can a person seek compensation for damages?	45
What is an offence under <i>PHIPA</i> ?	45
What are the consequences for committing an offence under <i>PHIPA</i> ?	46
Who is responsible for prosecuting offences under <i>PHIPA</i> ?	46

INTRODUCTION

WHAT IS THE *PERSONAL HEALTH INFORMATION PROTECTION ACT* AND WHY IS IT NECESSARY?

The *Personal Health Information Protection Act (PHIPA)* is Ontario's health-specific privacy legislation which came into force on November 1, 2004. *PHIPA* governs the manner in which personal health information may be collected, used and disclosed within the health sector. It regulates health information custodians (custodians), as well as individuals and organizations that receive personal health information from custodians.

Personal health information is among the most sensitive of personal information. People are understandably protective about sharing personal details relating to their medical conditions. At the same time, personal health information must flow freely between health care practitioners in order to ensure the best care for patients.

The nature of our health system is that personal health information passes through many links in the health care chain: from a doctor's office, to a referral to a specialist, to a medical lab, to a hospital or to an insurance company for reimbursement of claims. There are many circumstances in which personal health information must be readily, as well as expeditiously shared, such as in the case of a medical emergency. Beyond patient care, personal health information is needed for important activities, such as health research which is vital to develop new treatments and cures.

PHIPA creates a consistent approach to protecting personal health information across the health sector. The legislation was designed to give individuals greater control over how their personal health information is collected, used or disclosed. *PHIPA* balances the privacy rights of individuals with the legitimate need of custodians to collect, use and disclose personal health information in order to deliver effective and timely health care and to plan and manage our publicly funded health system.

With limited exceptions, *PHIPA* requires custodians to obtain consent before personal health information is collected, used or disclosed. In addition, *PHIPA* provides individuals with a right to access and request correction of their personal health information. *PHIPA* also provides a means for redress through the Office of the Information and Privacy Commissioner of Ontario (IPC) when privacy rights relating to personal health information have been violated.

What is the
*Personal Health
Information
Protection Act*
and why is it
necessary?

The IPC is the designated oversight body responsible for administering and enforcing these health sector privacy rules. As such, we have prepared the following questions and answers to guide Ontarians and custodians in understanding their respective privacy rights and obligations.

OVERVIEW

WHAT IS THE PURPOSE OF *PHIPA*?

PHIPA establishes rules for the collection, use and disclosure of personal health information and includes provisions that:

- require consent for the collection, use and disclosure of personal health information, with necessary but limited exceptions,
- require that custodians treat all personal health information as confidential and keep it secure,
- provide individuals with a right of access to their personal health information, as well as the right to correct errors,
- give individuals the right to withhold or withdraw consent to the collection, use or disclosure of personal health information or to expressly instruct custodians not to use or disclose their personal health information for health care purposes,
- establish clear rules for the collection, use and disclosure of personal health information for fundraising and marketing purposes,
- set guidelines for the collection, use and disclosure of personal health information for research purposes,
- ensure accountability by granting individuals the right to complain to the IPC about the practices of custodians and
- establish remedies for breaches of the legislation.

WHAT RIGHTS DO INDIVIDUALS HAVE?

PHIPA gives individuals the right to:

- be informed of the purposes for the collection, use and disclosure of personal health information,
- be notified by a custodian if personal health information has been stolen, lost or accessed by unauthorized persons,
- refuse or give consent to the collection, use or disclosure of personal health information, except in circumstances specified in *PHIPA*,

What rights do individuals have?

- withdraw consent by providing notice to the custodian,
- expressly instruct a custodian not to use or disclose personal health information for health care purposes without consent,
- access a copy of their own personal health information, except in limited circumstances specified in *PHIPA*,
- request corrections to be made to their personal health information,
- complain to the IPC about a custodian's refusal to give access to all or part of a record of personal health information,
- complain to the IPC about a custodian's refusal to grant a correction request,
- complain to the IPC about any breach or potential breach of *PHIPA* or its regulations and
- begin a proceeding in court for damages for actual harm suffered, if affected by a final order or conduct leading to a final conviction for an offence under *PHIPA*.

PHIPA establishes a formal process for individuals to access and correct their personal health information, within specified time frames and the right to complain if an access or correction request is denied.

WHAT IS THE RELATIONSHIP BETWEEN *PHIPA* AND THE FEDERAL *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)*?

The collection, use and disclosure of personal information within the commercial sector is regulated by federal privacy legislation—the *Personal Information Protection and Electronic Documents Act*. *PIPEDA* was enacted to regulate the collection, use or disclosure of personal information in the hands of private sector organizations. *PIPEDA* does not apply to personal information in provinces and territories that have “substantially similar” privacy legislation in place.

The federal government has deemed *PHIPA* to be “substantially similar” to *PIPEDA*. Custodians and their agents are exempted from having to comply with the provisions of *PIPEDA* to the extent that they collect, use and disclose personal health information within Ontario. *PIPEDA* continues to apply to all commercial activities relating to the exchange of personal health information between provinces and territories and to information transfers outside of Canada.

WHAT IS THE RELATIONSHIP BETWEEN *PHIPA*, THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA)* AND THE *MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (MFIPPA)*?

Organizations that are both custodians under *PHIPA* and institutions under public sector privacy and access to information legislation, namely the provincial *FIPPA* or its municipal counterpart *MFIPPA*, include hospitals, the Ontario Agency for Health Protection and Promotion, the Ministry of Health and Long-Term Care, medical officers of health and municipally operated long-term care homes and ambulance services.

The general rule is that, subject to certain exceptions, a custodian that is also an institution or a part of an institution is governed by *PHIPA*, not *FIPPA* or *MFIPPA*, with respect to personal health information in its custody or under its control. All other recorded information about an individual that is not personal health information and that is in the custody or under the control of an organization that is both a custodian and an institution or part of an institution is subject to *FIPPA* or *MFIPPA*, as the case may be.

PHIPA also contains provisions that are specific to custodians that are institutions. For example, *PHIPA* provides a number of exceptions to the general rule that custodians are only permitted to collect personal health information directly from the individual to whom the information relates. In addition to the exceptions available to all custodians, a custodian that is also an institution under *FIPPA* or *MFIPPA* may collect personal health information indirectly for a purpose related to investigating a breach of an agreement or a contravention or alleged contravention of laws of Ontario or Canada, the conduct of a proceeding or possible proceeding or the statutory function of the custodian.

For further information, please see the IPC documents *Applying PHIPA and FIPPA/MFIPPA to Personal Health Information, Freedom of Information at Ontario Hospitals: Frequently Asked Questions*, and *Applying PHIPA and FIPPA to Personal Health Information: Guidance for Hospitals*.

INTERPRETATION AND APPLICATION OF *PHIPA*

TO WHOM DOES *PHIPA* APPLY?

PHIPA applies to a wide variety of persons and organizations defined as health information custodians. *PHIPA* also applies to agents who are authorized to act for or on behalf of custodians. Additionally, *PHIPA* applies to the use and disclosure of personal health information by those who receive personal health information from custodians (recipients) and to electronic service providers, including health information network providers.

WHAT IS PERSONAL HEALTH INFORMATION?

Personal health information is “identifying information” about an individual, whether oral or recorded if the information:

- relates to the individual’s physical or mental condition, including family medical history,
- relates to the provision of health care to the individual,
- is a plan of service for the individual,
- relates to payments, or eligibility for health care or for coverage for health care,
- relates to the donation of any body part or bodily substance or is derived from the testing or examination of any such body part or bodily substance,
- is the individual’s health number or
- identifies a health care provider or a substitute decision-maker for the individual.

“Identifying information” includes information that identifies an individual or for which it is reasonably foreseeable that it could be used, either alone or with other information, to identify an individual.

Personal health information includes identifying information that is not personal health information but that is contained in a record that contains personal health information. Personal health information does not include identifying information

about an employee or agent of the custodian that is not maintained primarily for the provision of health care. For example, a doctor's note to support an absence from work in the personnel file of a secretary employed by a custodian is not personal health information.

What is
personal health
information?

WHAT DOES "HEALTH CARE" MEAN?

"Health care" means any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and that is carried out or provided:

- for diagnosis, treatment or maintenance of an individual's physical or mental condition,
- for prevention of disease or injury or the promotion of health or
- as part of palliative care.

It also includes:

- the compounding, dispensing or selling of a drug, device or equipment pursuant to a prescription,
- a community service that is described in the *Home Care and Community Services Act* and
- taking blood or a blood product donation from an individual.

WHAT IS A CUSTODIAN?

A custodian is a person or organization listed in *PHIPA* that, as a result of his, her or its power or duties or work set out in *PHIPA*, has custody or control of personal health information. Examples of custodians include:

- health care practitioners, (including doctors, nurses, speech-language pathologists, chiropractors, dental professionals, dieticians, medical laboratory technologists, massage therapists, midwives, occupational therapists, opticians and physiotherapists),
- community care access corporations,
- hospitals,
- psychiatric facilities,
- long-term care homes,

What is a custodian?

- pharmacies,
- laboratories,
- ambulance services,
- retirement homes and homes for special care,
- medical officers of health of boards of health,
- the Minister of Health and Long-Term Care and
- Canadian Blood Services.

A custodian does not include:

- a health care practitioner, service provider, evaluator or assessor who is an agent of a custodian,
- a person authorized to act for or on behalf of a person that is not a custodian, if the scope of duties of the authorized person does not include the provision of health care,
- an aboriginal healer who provides traditional healing services to aboriginal persons or members of an aboriginal community,
- an aboriginal midwife who provides traditional midwifery services to aboriginal persons or members of an aboriginal community and
- a person who provides treatment solely by spiritual means or by prayer.

IS A HEALTH CARE PRACTITIONER WORKING FOR A NON-CUSTODIAN CONSIDERED TO BE A CUSTODIAN?

A health care practitioner, who provides health care, but who contracts with, is employed by or volunteers for an organization that is not defined as a custodian under *PHIPA*, would fall within the definition of a custodian under *PHIPA* and must comply with all requirements for custodians.

Examples of custodians who work for non-custodians include:

- a nurse employed by a school board to provide health care services to students,
- a doctor employed by a professional sports team in order to diagnose sporting injuries,

- a registered massage therapist providing health care services to clients of a spa and
- a nurse employed in-house by a manufacturing firm in a health care capacity.

Is a health care practitioner working for a non-custodian considered to be a custodian?

A custodian cannot disclose personal health information to a non-custodian, including the non-custodian for whom the individual is working, unless the individual whose personal health information is at issue has given express consent or the disclosure is permitted or required by *PHIPA* or another law.

For further information, please see the IPC fact sheet, *Health Information Custodians Working for Non-Health Information Custodians*.

WHAT IS AN AGENT?

PHIPA defines an agent to include any person who is authorized by a custodian to perform services or activities in respect of personal health information on the custodian's behalf and for the purposes of that custodian.

An agent may include a person or company that contracts with, is employed by or volunteers for a custodian and, as a result, may have access to personal health information. *PHIPA* permits custodians to provide personal health information to their agents only if the custodian is permitted to collect, use, disclose, retain or dispose of the information.

For example, an agency relationship under *PHIPA* includes a nurse who is employed by, or a student who volunteers at, a hospital. An agency relationship may also include a physician who is not employed by a hospital, but has admitting privileges to use the hospital's equipment or facilities. In such cases, the custodian hospital is permitted to authorize the agent to handle or deal with personal health information on its behalf, as long as the agent complies with *PHIPA* and adopts the information practices of the custodian. An agent must notify the custodian if the personal health information the agent is handling is stolen, lost or accessed by unauthorized persons.

The custodian remains accountable for the personal health information in its custody or under its control, even where the agent is authorized to act on its behalf with respect to that personal health information. The custodian also remains accountable for the personal health information in its custody or under its control where the agent acted beyond what was authorized by the custodian. For example, in Order HO-013, employees were found to be agents when they used and/or disclosed personal health information in the custody or under the control of a hospital for the purpose of selling or marketing Registered Education Saving Plans. The custodian hospital was accountable for the contravention of *PHIPA*, even though the agents may have acted beyond the authority delegated by the hospital.

DOES *PHIPA* APPLY TO INSURANCE COMPANIES OR EMPLOYERS?

Certain organizations, such as insurance companies and employers, who may hold personal health information in their files, are not governed by *PHIPA*, unless they receive personal health information from a custodian. When an insurance company or employer receives personal health information from a custodian, the receiving entity may, in general, only use or disclose the information for the authorized purpose for which the information was disclosed or for the purpose of carrying out a statutory or legal duty. This rule is colloquially referred to as the “recipient rule.”

However, an exception to the recipient rule applies to insurance providers that receive personal health information from a pharmacist. In that situation, *PHIPA* permits the insurance provider to disclose personal health information to the pharmacist to assist the pharmacist in advising the individual or providing the individual with health care. For example, the insurance provider may disclose to a pharmacist the types of medications an individual has purchased from different pharmacies so that the pharmacist may advise of any incompatible prescriptions.

WHAT IS AN ELECTRONIC SERVICE PROVIDER?

An electronic service provider is a person who supplies services that enable a custodian to collect, use, modify, disclose, retain or dispose of personal health information electronically. If the electronic service provider is not an agent of the custodian, then it shall not use any personal health information to which it has access in the course of providing services to the custodian, except as necessary in the course of providing the service and it cannot disclose the information. Electronic service providers must also ensure their employees or any other persons acting on their behalf agree to comply with these restrictions.

WHAT IS A HEALTH INFORMATION NETWORK PROVIDER?

PHIPA contains requirements that apply to a specific type of electronic service provider, referred to as a health information network provider. A health information network provider is a person who provides services to two or more custodians, where the services are provided primarily to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians. Among other requirements, health information network providers must:

- notify the custodian of any breaches,
- perform threat risk assessments and privacy impact assessments,
- upon request, provide an electronic record to the custodian of all accesses and transfers of the personal health information,
- ensure that retained third parties comply with necessary restrictions and conditions,
- enter into a written agreement with the custodian and
- make publicly available information about its services to the custodian.

WHO IS A PRESCRIBED PERSON?

The regulations prescribe a list of persons who compile and maintain registries of personal health information for the purpose of facilitating or improving the provision of health care or that relates to the storage or donation of bodily parts or substances. Custodians are permitted to disclose personal health information without consent to these listed persons. They consist of the following:

- Cardiac Care Network of Ontario in respect of its registry of cardiac services,
- INSCYTE (Information System for Cytology etc.) Corporation in respect of CytoBase,
- Hamilton Health Sciences Corporation in respect of the Critical Care Information System,
- Cancer Care Ontario in respect of the Ontario Cancer Screening Registry,
- Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network and
- Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank.

The above-noted prescribed persons may use and disclose personal health information for the purpose of facilitating or improving the provision of health care or for the storage or donation of bodily parts or substances. They are also permitted to use and disclose personal health information for research purposes, with a research plan approved by a research ethics board (REB) in certain circumstances. These prescribed persons are also permitted to disclose personal health information to prescribed entities for the planning, management or analysis of the health system.

Who is a prescribed person?

The regulations also require that prescribed persons make publicly available:

- a plain language description of the functions of the registry and
- a summary of the practices and procedures to protect the privacy of the individuals whose personal health information they receive and to maintain the confidentiality of the information.

The prescribed person must have its practices and procedures approved by the IPC every three years.

For further information, please see the IPC's *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

WHAT IS A PRESCRIBED ENTITY?

The regulations prescribe a list of entities, including any registries maintained within these listed entities, that custodians are permitted to disclose personal health information to without consent for purposes of planning, management and analysis of the health system. Prescribed entities consist of the following:

- Cancer Care Ontario,
- Canadian Institute for Health Information,
- Institute for Clinical Evaluative Sciences and
- Pediatric Oncology Group of Ontario.

In certain circumstances, with a research plan approved by a research ethics board, these prescribed entities are permitted to use and disclose personal health information for research purposes as if they were custodians. A prescribed entity is permitted to disclose personal health information to a prescribed person who compiles or maintains a registry of personal health information, and to another prescribed entity for purposes related to the planning, management and analysis of the health system.

The regulations also require that prescribed entities make publicly available:

- a plain language description of the functions of the entity and
- a summary of the practices and procedures to protect the privacy of the individuals whose personal health information they receive and to maintain the confidentiality of the information.

The prescribed entity must have its practices and procedures approved by the IPC every three years.

For further information, please see the IPC's *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

PRACTICES TO PROTECT PERSONAL HEALTH INFORMATION

HOW DOES *PHIPA* PROTECT PERSONAL HEALTH INFORMATION?

PHIPA establishes certain privacy rights for individuals and imposes specific obligations on custodians in protecting personal health information. Custodians who have custody or control of personal health information must develop and implement information practices that comply with the requirements of *PHIPA*. Custodians must also ensure that personal health information is as accurate, up-to-date and complete as is necessary for the purposes for which they use or disclose personal health information.

PHIPA requires custodians to take steps that are reasonable in the circumstances to ensure personal health information in their custody or under their control is protected against theft, loss and unauthorized use and disclosure, and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal.

PHIPA also requires custodians to ensure that records of personal health information are retained, transferred and disposed of in a secure manner. According to the definition of “disposed of in a secure manner” in the regulations, records of personal health information must be destroyed in such a manner that their reconstruction is not reasonably foreseeable.

PHIPA requires records of personal health information to be kept for as long as needed to allow an individual to exhaust any legal recourse regarding an access request. As *PHIPA* does not establish specific retention periods for personal health information, custodians should refer to their governing legislation to determine applicable record retention requirements. For example, regulations under the *Public Hospitals Act* specify how long hospitals must retain records of personal health information.

For further information, please see the IPC fact sheets, *Safeguarding Personal Health Information*, *Secure Destruction of Personal Health Information*, *Encrypting Personal Health Information on Mobile Devices*, *Health-Care Requirement for Strong Encryption* and *The Secure Transfer of Personal Health Information*, and the IPC discussion papers *Get Rid of it Securely to keep it Private – Best Practices for the Secure Destruction of Personal Health Information* and *Detecting and Detering Unauthorized Access to Personal Health Information*.

WHAT ARE THE NOTIFICATION REQUIREMENTS IN *PHIPA* IN THE EVENT OF A BREACH?

PHIPA contains notification requirements for both agents and custodians. If personal health information handled by an agent on behalf of a custodian is stolen, lost or accessed by unauthorized persons, the agent must notify the custodian of the breach at the first reasonable opportunity. *PHIPA* also requires custodians to notify individuals at the first reasonable opportunity if personal health information is stolen, lost or accessed by an unauthorized person. However, a custodian who is a researcher and received personal health information for research purposes from another custodian must not notify an individual, unless the researcher is informed that the individual has given consent to being contacted.

For further information please see the IPC guidelines, *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*.

DO CUSTODIANS HAVE RESPONSIBILITIES WITH RESPECT TO ACCOUNTABILITY AND OPENNESS?

In order to enhance transparency, *PHIPA* contains specific requirements for custodians that relate to accountability and openness. For example, a custodian must designate a contact person who is authorized on behalf of the custodian to facilitate compliance with *PHIPA*, ensure agents are appropriately informed of their duties, respond to inquiries about the custodian's information practices, respond to access and correction requests and receive complaints from the public. A custodian that is a natural person may designate a contact person, or else perform the functions on their own.

A custodian must also provide a written statement that is readily available to the public and describes the custodian's information practices, how to reach the contact person, how to obtain access to or request a correction of a record of personal health information and how to make a complaint to the custodian and to the IPC.

Unless an individual does not have a right of access, a custodian must notify the individual of any uses and disclosures of personal health information that occur without the individual's consent in a manner that is outside of the scope of the custodian's description of its information practices. The custodian must also make a note of these uses and disclosures and keep the note as a part of, or linked to, the records of personal health information.

WHAT ARE THE REQUIREMENTS FOR THE TREATMENT OF PERSONAL HEALTH RECORDS IN THE EVENT OF A CHANGE IN PRACTICE?

A change in practice occurs in a variety of circumstances, for example, due to death, bankruptcy, retirement or relocation. It is important to identify who the custodian of records of personal health information is in the event of a planned or unforeseen change in practice. Generally, a custodian remains a custodian with respect to a record of personal health information until complete custody and control of the record passes to another person who is legally authorized to hold it.

Upon the death of a custodian, the estate trustee or the person who assumed responsibility for the administration of the estate becomes the custodian, until custody and control passes to another person who is legally authorized to hold the records. If another person, for example a trustee in bankruptcy, obtains complete custody or control of the records as a result of the bankruptcy or insolvency of the custodian, then that person becomes the custodian. A custodian may also divest itself of responsibility for records by transferring them to an archive.

When complete custody or control of the records is transferred to a successor, then the successor becomes the custodian. The original custodian must make reasonable efforts to notify the individual to whom the personal health information relates before the transfer to the successor, or, if that is not reasonably possible, as soon as possible after transferring the records.

If none of the above conditions apply, then the existing custodian of the records remains the custodian. *PHIPA* requires custodians to protect personal health information and to ensure that records of personal health information are retained, transferred and disposed of in a secure manner. A custodian remains responsible for records of personal health information even where the records are being retained by an agent of the custodian, such as a record storage company.

For further information, please see the IPC documents *How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice* and *Checklist for Health Information Custodians in the Event of a Planned or Unforeseen Change in Practice*.

CONSENT CONCERNING PERSONAL HEALTH INFORMATION

WHAT ARE THE REQUIREMENTS FOR CONSENT?

The general rule is that a custodian needs to obtain an individual's consent to collect, use and disclose personal health information, unless *PHIPA* allows the collection, use or disclosure without consent. An individual's consent may be express or implied. Under *PHIPA*, regardless of whether it is express or implied, consent must be:

- knowledgeable,
- voluntary (not obtained through deception or coercion),
- related to the information in question and
- given by the individual.

Knowledgeable consent means that it is reasonable in the circumstances to believe that an individual knows why a custodian collects, uses and discloses their personal health information and that they may give or withhold this consent.

A custodian may ensure that consent is knowledgeable by posting or making readily available a notice that is likely to come to the individual's attention, describing the purposes for the collection, use and disclosure of personal health information.

WHAT IS THE DIFFERENCE BETWEEN EXPRESS AND IMPLIED CONSENT?

Express consent to the collection, use or disclosure of personal health information by a custodian is consent that has been clearly and unmistakably given. Express consent may be explicitly provided, either orally or in writing.

Implied consent to the collection, use or disclosure of personal health information is consent that a custodian concludes has been given based on an individual's action or inaction in particular factual circumstances.

For example, when an individual discloses their personal health information for the purposes of filling out a prescription, a pharmacist can reasonably infer consent to the collection of that information.

What is the difference between express and implied consent?

WHEN IS EXPRESS CONSENT REQUIRED?

Subject to very limited exceptions, express consent is required:

- where personal health information is disclosed to a person or an organization, such as an insurance company, that is not a custodian and
- where information is disclosed by one custodian to another for a purpose other than providing or assisting in providing health care.

Express consent is also required where a custodian:

- collects, uses or discloses personal health information other than an individual's name and mailing address for fundraising purposes,
- collects, uses or discloses personal health information for marketing or marketing research and
- collects, uses or discloses personal information for research purposes, unless certain conditions and restrictions are met.

WHEN IS IMPLIED CONSENT SUFFICIENT?

In practice, a custodian is not required to obtain an individual's written or verbal consent every time personal health information is collected, used or disclosed. Custodians may rely on the implied consent of an individual to collect and use personal health information for most purposes. They may also infer consent to disclose personal health information to another custodian for the purposes of providing or assisting in providing health care. Subject to limited exceptions, custodians cannot rely on implied consent when disclosing personal health information to a person or organization that is not a custodian, or when disclosing personal health information for a purpose other than providing or assisting in providing health care.

Subject to additional requirements and restrictions, implied consent is permitted if a custodian collects, uses or discloses names or mailing addresses for the purposes of fundraising. In addition, if individuals have provided information about their religious affiliation to a health care facility, the facility may rely on implied consent to provide the individual's name and location within the facility to a person representing their religious organization. Before making this

When is implied consent sufficient?

disclosure, the facility must provide the individual with an opportunity to withhold or withdraw consent. A health care facility may also disclose to a person the fact that an individual is a patient or resident in the facility, the individual's general health status, and the location of the individual, if the individual is offered the option, at the first reasonable opportunity after admission to the facility, to object to such disclosures and does not do so.

PHIPA distinguishes between implied consent and assumed implied consent. In the case of implied consent, custodians must ensure that all the required elements of consent are fulfilled; whereas in the case of assumed implied consent, custodians may assume that all the elements of consent are fulfilled, unless it is not reasonable to do so in the circumstances.

WHAT IS THE 'CIRCLE OF CARE'?

The "circle of care" is not a defined term under *PHIPA*. It is a term of reference used to describe the provisions of *PHIPA* that enable custodians to rely on an individual's assumed implied consent when collecting, using or disclosing personal health information for the purpose of providing or assisting in providing health care. For example:

- With respect to a physician's office, the circle of care may include: the physician, a nurse, a specialist or other health care practitioner referred by the physician and any other health care practitioner selected by the patient, such as a pharmacist or physiotherapist.
- In the context of a hospital, the circle of care may include: the attending physician and the health care team, for example residents, nurses, clinical clerks and employees assigned to the patient, who have the responsibility of providing care to the individual or assisting with that care. The circle of care could also include, among others, custodians, external to the hospital, who will be involved in providing health care to the patient upon discharge from the hospital.

The circle of care does not include:

- custodians who are not part of the direct or follow-up treatment of an individual and
- non-custodians, for example, insurance companies.

WHEN CAN CUSTODIANS ASSUME IMPLIED CONSENT?

In order to rely on assumed implied consent to collect, use or disclose personal health information, the custodian must first fall within a category of custodians that are entitled to rely on assumed implied consent. Most custodians, such as health care practitioners, hospitals, pharmacies, long-term care homes and community care access centres, can rely on assumed implied consent. However, some custodians are not entitled to assume implied consent. For example, these include:

- an evaluator under the *Health Care Consent Act*,
- an assessor under the *Substitute Decisions Act, 1992*,
- the Minister or Ministry of Health and Long-Term Care and
- Canadian Blood Services.

In order for a custodian to rely on assumed implied consent a number of other requirements must also be fulfilled, including:

- The personal health information to be collected, used or disclosed by the custodian must be received from the individual, the substitute-decision maker or another custodian.
 - For example, a custodian may not rely on assumed implied consent if the personal health information was received from an employer, insurance provider or educational institution.
- The custodian must have received the personal health information that is being collected, used or disclosed for the purpose of providing or assisting in the provision of health care to the individual.
 - A custodian may not rely on assumed implied consent if the personal health information was received for other purposes such as research, fundraising, marketing or providing or assisting in the provision health care to another individual or group of individuals.
- The purpose of the collection, use or disclosure of personal health information by the custodian must be for the provision of health care or assisting in the provision of health care to the individual.
 - A custodian may not rely on assumed implied consent if the collection, use or disclosure is for other purposes, such as research, fundraising, marketing or providing or assisting in the provision of health care to another individual or group of individuals.

When can custodians assume implied consent?

- In the context of disclosure, the disclosure of personal health information by the custodian must be to another custodian.
- The custodian that receives the personal health information must not be aware that the individual have expressly withheld or withdrawn consent to the collection, use or disclosure.

For further information, please see the IPC guidance document *Circle of Care: Sharing Personal Health Information for Health-Care Purposes*.

ARE PHARMACISTS REQUIRED TO OBTAIN EXPRESS CONSENT FROM AN INDIVIDUAL TO DISCLOSE PERSONAL HEALTH INFORMATION TO A THIRD PARTY BENEFITS PAYOR?

No. The regulations provide an exception to the express consent requirement where a pharmacist discloses personal health information to a third party who is not a custodian and who is being asked to provide payment for a medication or related goods or services provided to an individual. Pharmacists are permitted to rely on an individual's implied consent as long as they are satisfied that all the required elements of consent are fulfilled.

CAN INDIVIDUALS CONTROL WHAT PERSONAL HEALTH INFORMATION IS RECORDED IN THEIR FILE?

Yes, but any condition placed on the collection, use or disclosure of personal health information cannot prohibit or restrict the recording of personal health information that is required by law or by established standards of professional or institutional practice.

CAN INDIVIDUALS WITHDRAW THEIR CONSENT?

Yes. An individual may, with limited exceptions, withdraw consent at any time for the collection, use or disclosure of personal health information by providing notice to the custodian. This applies to implied, as well as express consent.

A withdrawal of consent is not retroactive. For example, this means that where a disclosure has been made on the basis of consent, the custodian is not required to retrieve the information that has already been disclosed. However, the custodian must stop disclosing the personal health information as soon as

the notice of withdrawal is received. A withdrawal of consent would not apply to a collection or use that had already occurred prior to receiving the notice of withdrawal. It would only apply to new collections of personal health information and future uses for the purpose of which the consent was initially obtained.

Can individuals withdraw their consent?

WHAT IS A 'LOCK-BOX'?

The “lock-box” is not a defined term under *PHIPA*. It is a term commonly used to describe the right of individuals to withhold or withdraw their consent to the collection, use or disclosure of their personal health information for health care purposes. Individuals may expressly instruct custodians not to use or disclose their personal health information for health care purposes without consent, where *PHIPA* would otherwise permit a use or disclosure for such a purpose.

The withholding or withdrawal of consent or the express instructions may take various forms, including communications from individuals to custodians: not to collect, use or disclose a particular item of personal health information, such as a specific diagnosis, for health care purposes, not to collect, use or disclose the contents of their entire record of personal health information for health care purposes and/or not to use and/or disclose their personal health information to a particular custodian, a particular agent of a custodian or to a class of custodians or agents, for example, physicians, nurses or social workers, for health care purposes.

WHAT ARE THE RESTRICTIONS AND LIMITATIONS ON THE LOCK-BOX?

Once an individual locks personal health information, a custodian subject to the withdrawal or withholding of consent or express instruction cannot collect, use or disclose, as the case may be, that personal health information for health care purposes, unless the individual provides express consent and informs the custodian accordingly or unless *PHIPA* otherwise permits the collection, use or disclosure to be made without consent. For example, the custodian is permitted to disclose the locked personal health information where the custodian believes, on reasonable grounds, that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to an individual or a group of persons.

Further, an individual’s restriction may not impede a custodian from recording personal health information about an individual that is required by law or by established standards of professional or institutional practice.

What are the restrictions and limitations on the lock-box?

If a custodian discloses an individual's personal health information to another custodian for the provision of health care and the disclosing custodian does not have consent to disclose all the personal health information that it considers reasonably necessary for that purpose, the disclosing custodian must notify the receiving custodian of that fact. The receiving custodian would then be able to explore the matter of the locked personal health information with the individual and seek their express consent to access the locked information.

For further information, please see the IPC fact sheet, *Lock-Box Fact Sheet*.

WHAT HAPPENS WHEN AN INDIVIDUAL IS INCAPABLE OF PROVIDING CONSENT?

Under *PHIPA*, individuals are presumed to be capable of making their own decisions regarding the collection, use or disclosure of their personal health information. Individuals are capable of consent if they are able to understand information relevant to deciding whether to consent to the collection, use or disclosure of their personal health information, and to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing their consent.

If a custodian believes that an individual is incapable of providing consent, *PHIPA* permits a substitute decision-maker, such as a relative, spouse, child's parent, or the Public Guardian and Trustee, to make a decision on an individual's behalf.

PHIPA lists, in order of priority, the following substitute decision-makers who may consent on behalf of an individual when consent is required, including:

- a substitute decision-maker within the meaning of section 9, section 39 and section 56 of the *Health Care Consent Act*, if the purpose of the collection, use or disclosure is necessary for, or ancillary to, a decision about a treatment under Part II, a decision about admission to a care facility under Part III or a decision about a personal assistance service under Part IV of the *Health Care Consent Act* respectively,
- the attorney for personal care or for property,
- the representative appointed by the Consent and Capacity Board,
- the spouse or partner,
- a child or parent, including a children's aid society,
- a parent who has a right of access,

- a sibling,
- a relative and if no other person meets the requirements
- the Public Guardian and Trustee.

CAN A CHILD UNDER 16 YEARS OLD PROVIDE CONSENT?

A custodian may obtain consent for the collection, use and disclosure of personal health information from a capable child, regardless of age. As discussed above, individuals are capable of consent if they are able to understand information relevant to deciding whether to consent to the collection, use or disclosure of their personal health information, and to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing their consent.

If the child is less than 16 years old, a parent of the child or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent may also give, withhold or withdraw consent. However, this does not apply in the context of information that relates to treatment within the meaning of the *Health Care Consent Act*, about which children have made a decision on their own, or counselling in which children have participated on their own under the *Child and Family Services Act*. A parent does not include a parent who has only a right of access to the child. If there is a conflict between a capable child who is less than 16 years old, and the person who is entitled to act as the child's substitute decision-maker, the decision of the capable child regarding giving, withholding or withdrawing consent prevails.

CAN ANOTHER PERSON, SUCH AS A FAMILY MEMBER, PROVIDE CONSENT ON AN INDIVIDUAL'S BEHALF WHEN PICKING UP OR DROPPING OFF A PRESCRIPTION?

Yes. The regulations permit a pharmacist to provide a prescription to another person. This is also permitted under the *Drug and Pharmacies Regulation Act*.

COLLECTION, USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION

WHAT ARE THE GENERAL LIMITATIONS ON THE COLLECTION, USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION?

A custodian is prohibited from collecting, using or disclosing personal health information unless consent has been obtained and the collection, use and disclosure is, to the best of the custodian's knowledge, necessary for a lawful purpose or is permitted or required by *PHIPA*.

According to *PHIPA*, a custodian must not collect, use or disclose personal health information if other information will serve the purpose of the collection, use or disclosure. For example, a custodian may be able to provide a researcher conducting a study with de-identified information, rather than disclosing personal health information. A custodian must not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure. For example, if a patient requests a doctor's note to give to the employer, the doctor should only include the minimum information necessary, rather than the patient's entire health history.

COLLECTION

WHAT IS A COLLECTION OF PERSONAL HEALTH INFORMATION UNDER *PHIPA*?

PHIPA defines the term "collect" as the gathering, acquiring, receiving or obtaining of personal health information by any means from any source. This means that personal health information can be collected by a custodian or an authorized agent under *PHIPA* in several ways, such as when a doctor makes notes about a patient or when a pharmacist receives a prescription to be filled.

WHAT ARE THE RULES REGARDING THE COLLECTION OF PERSONAL HEALTH INFORMATION?

As a general rule, consent is required for any collection of an individual's personal health information, unless *PHIPA* allows the collection without consent. Custodians within the "circle of care" may rely on an individual's implied consent, or assumed implied consent if the requirements are fulfilled, to collect personal health information for the purpose of providing health care.

With limited exceptions, custodians must collect personal health information directly from the individual involved. Custodians must not collect personal health information if other information will serve the purpose of the collection and may only collect as much information as is necessary to meet the purpose of collection.

WHEN CAN CUSTODIANS INDIRECTLY COLLECT PERSONAL HEALTH INFORMATION?

Custodians may collect personal health information indirectly where, for example:

- the individual consents,
- the collection is necessary for providing health care and it is not possible to collect personal health information directly from the individual that can be relied on as accurate and complete,
- the collection is necessary for providing health care and it is not possible to collect personal health information directly from the individual in a timely manner,
- the custodian collects personal health information for the purposes of research from a person who is not a custodian, provided that certain conditions are met,
- the indirect collection is required or permitted by law,
- the custodian is a prescribed entity and is collecting personal health information from a person who is not a custodian for the purposes of the planning and management of the health system or
- the IPC authorizes the indirect collection.

USE

WHAT IS A USE OF PERSONAL HEALTH INFORMATION UNDER *PHIPA*?

The term “use” in relation to personal health information in the custody or under the control of a custodian or a person, is defined under *PHIPA* as meaning to handle or deal with personal health information, but does not include to disclose the information. Where a custodian is authorized to use the information, the custodian may provide the information to an agent of the custodian to use it for that purpose on behalf of the custodian. The sharing of information between a custodian and its agent is considered to be a use and not a disclosure or a collection for the purposes of *PHIPA*. Order HO-013 found that handling and dealing with personal health information includes accessing/viewing personal health information.

WHAT ARE THE RULES REGARDING THE USE OF PERSONAL HEALTH INFORMATION?

As a general rule, consent is required for any use of an individual’s personal health information, unless *PHIPA* allows the use without consent. Custodians must not use personal health information if other information will serve the purpose of the use, and may only use as much information as is necessary to meet the purpose of the use of personal health information.

When using personal health information, a custodian must take reasonable steps to ensure that the individual’s personal health information is as accurate, complete and up-to-date as is necessary for the purposes for which the custodian uses the information.

WHEN CAN PERSONAL HEALTH INFORMATION BE USED WITHOUT CONSENT?

PHIPA sets out a limited set of acceptable uses of personal health information without consent, including, for example, the following purposes:

- planning or delivering programs or services,
- risk management, error management or activities to improve or maintain the quality of care or any related program or service,
- educating agents to provide health care,

- obtaining payment or processing, monitoring, verifying or reimbursing health care claims,
- research, provided that specific requirements and conditions are met and
- If permitted or required by law.

When can personal health information be used without consent?

A custodian may provide personal health information to an agent of the custodian for any of these purposes.

DISCLOSURE

WHAT IS A DISCLOSURE OF PERSONAL HEALTH INFORMATION UNDER *PHIPA*?

The term “disclose” in relation to personal health information in the custody or under the control of a custodian or a person, is defined under *PHIPA* as meaning to make the personal health information available or to release it to another custodian or person. It does not include providing personal health information back to the person who provided it or disclosed it in the first place, whether or not the personal health information has been manipulated or altered, as long as it does not include additional identifying information.

WHAT ARE THE RULES REGARDING THE DISCLOSURE OF PERSONAL HEALTH INFORMATION?

As a general rule, consent is required to disclose an individual’s personal health information, unless *PHIPA* allows the disclosure without consent. Custodians must not disclose personal health information if other information will serve the purpose of the disclosure, and may only disclose as much information as is necessary to meet the purpose.

A custodian and its authorized agents may rely on implied consent, or assumed implied consent if the requirements are fulfilled, for the disclosure of personal health information within the “circle of care” while providing health care, as long as the disclosure is reasonably necessary for the provision of health care, and the individual has not expressly withheld or withdrawn consent.

PHIPA permits custodians to disclose personal health information in certain limited situations. However, simply because a disclosure is permitted does not mean it is mandatory, unless it is necessary to carry out a statutory or legal duty.

What are the rules regarding the disclosure of personal health information?

Unless permitted or required by law, express consent is generally required when personal health information is disclosed by a custodian to a non-custodian, where a custodian discloses to another custodian for a purpose other than for health care or for market research, unless specific conditions are met and fundraising, if more than contact information is provided.

When disclosing personal health information, the custodian should take care to ensure that no information is inadvertently disclosed to third parties.

WHEN CAN PERSONAL HEALTH INFORMATION BE DISCLOSED WITHOUT CONSENT?

PHIPA recognizes the need for a flexible approach to regulating information exchanges between custodians in order to ensure the effective and efficient operation of the health system. Consequently, custodians may disclose personal health information without an individual's consent in certain circumstances. While these disclosures without consent are permitted by *PHIPA*, they are not mandatory, unless they are necessary to carry out a statutory or legal duty. Examples of permitted disclosures of personal health information without consent include:

- if the disclosure is reasonably necessary for providing health care and consent cannot be obtained in a timely manner, unless there is an express request from the individual instructing otherwise,
- in order for the Minister of Health and Long-Term Care to provide funding to the custodian for the provision of health care,
- for the purpose of contacting a relative or friend or potential substitute decision-maker of an individual who is injured, incapacitated or ill and unable to give consent personally,
- to inform any person that an individual is a patient or resident in a facility, the individual's general health status, and the location of the individual in the facility, unless there is an express request from the individual instructing otherwise,
- to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons,
- when transferring records to the archives for conservation,
- for the purpose of carrying out an inspection, investigation or similar procedure that is authorized by a warrant, *PHIPA* or another *Act*,

- for determining or verifying eligibility for publicly funded health care or related goods, services or benefits,
- for the purpose of administration and enforcement of various *Acts* by the professional Colleges and other regulatory bodies,
- to a prescribed person, listed in the regulations, that compiles and maintains a registry of personal health information for the purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances,
- to a prescribed entity, listed in the regulations, for the purpose of analysis or compiling information with respect to the management, evaluation or monitoring of the health system,
- to the Public Guardian and Trustee, a children’s aid society and the Children’s Lawyer for the purpose of carrying out their statutory functions,
- to a person conducting an audit or reviewing an accreditation or application for accreditation related to the services of a custodian,
- for the purpose of legal proceedings, in specific circumstances,
- for the purpose of research, subject to restrictions and conditions and
- for any purpose as required or permitted by law.

CAN PERSONAL HEALTH INFORMATION BE DISCLOSED IN THE EVENT OF AN EMERGENCY?

PHIPA does not prevent the rapid sharing of personal health information in certain situations. *PHIPA* is not intended to stand in the way of the disclosure of vital—and in some cases, life-saving—information in emergency or critical situations affecting individuals or public health and safety, as well as in situations that call for compassion.

Personal health information may be disclosed without consent if the custodian believes on reasonable grounds that the disclosure is necessary for eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. For example, a psychologist at a university could disclose a student’s personal health information to the student’s family or physician, if the psychologist believes it is necessary to reduce the risk of suicide. *PHIPA* also allows a custodian to disclose personal health information without consent in order to contact a relative, friend or potential substitute decision-maker if an individual is injured, incapacitated or ill and unable to consent.

Can personal health information be disclosed in the event of an emergency?

Custodians may also disclose personal health information if permitted or required by another law. For example, the *Health Protection and Promotion Act (HPPA)* requires certain custodians to report diseases defined as reportable, communicable or virulent to the Medical Officer of Health. *PHIPA* also provides that custodians may disclose personal health information without consent to the Chief Medical Officer of Health or to a local medical officer of health for the purposes of the *HPPA* and to the Ontario Agency for Health Protection and Promotion for the purposes of the *Ontario Agency for Health Protection and Promotion Act*. For example, a custodian may report an outbreak of a suspicious condition that is not identified as a reportable, communicable or virulent disease, but which the custodian believes could be dangerous.

For further information, please see the IPC fact sheet, *Disclosure of Information Permitted in Emergency or other Urgent Circumstances*.

DOES *PHIPA* PERMIT DISCLOSURE OF PERSONAL HEALTH INFORMATION ABOUT A DECEASED INDIVIDUAL?

PHIPA permits the disclosure of personal health information about a deceased individual in certain circumstances. A custodian may only disclose personal health information to a person who is not a custodian, such as a relative of a deceased individual, if the individual whose personal health information is at issue, has given express consent or the disclosure is permitted or required by *PHIPA* or another law. In the case of a deceased individual, the consent may be given by the deceased individual's substitute decision-maker. This means that if the substitute decision-maker consents, the personal health information may be disclosed to a relative of the deceased individual.

PHIPA permits, but does not require, a custodian to disclose personal health information without consent for the purposes of identifying the individual or for informing people whom it is reasonable to inform, that the individual is deceased or reasonably suspected to be deceased and the circumstances of death, where appropriate. *PHIPA* also permits disclosure to the spouse, partner, sibling or child of the deceased individual if the recipients reasonably require the information to make decisions about their own, or their children's health care.

For further information, please see the IPC fact sheet, *Obtaining Personal Health Information About a Deceased Relative*.

CAN A CUSTODIAN DISCLOSE PERSONAL HEALTH INFORMATION TO THE WORKPLACE SAFETY AND INSURANCE BOARD (WSIB) ABOUT AN INJURED WORKER WITHOUT THE INDIVIDUAL'S CONSENT?

Yes. *PHIPA* permits the disclosure of personal health information without consent, if permitted or required by another law. For example, this means that *PHIPA* does not interfere with the *Workplace Safety and Insurance Act (Act)*, where that *Act* requires a hospital or health facility, which provides health care to a worker claiming benefits under the insurance plan, to give the WSIB such information relating to the worker as the WSIB may require. This requirement also applies to a health care practitioner who provides health care to a worker or is consulted with respect to a worker's health care. When requested to do so by an injured worker or the employer, the *Act* requires a health care practitioner treating the worker to give the WSIB, the worker and the employer prescribed information concerning the worker's functional abilities.

PHIPA also does not interfere with the *Occupational Health and Safety Act*, which sets out an employer's and supervisor's duty, subject to specific limitations, to provide a worker with information, including personal information, related to a risk of workplace violence from a person with a history of violent behaviour.

CAN A CUSTODIAN STORE, ACCESS OR DISCLOSE PERSONAL HEALTH INFORMATION OUTSIDE OF ONTARIO?

PHIPA does not require that personal health information be retained and stored in Ontario or Canada. There is no legislative prohibition on storing and accessing personal health information outside of Ontario. For example, a custodian may decide to outsource the storage of personal health information to a service provider in another jurisdiction. However, the custodian is ultimately accountable for the actions of its agent and must be satisfied that appropriate administrative, physical and technical safeguards are in place, for example, through contractual arrangements.

PHIPA permits disclosures of personal health information to a person outside of Ontario in certain situations. A custodian may disclose personal health information about an individual collected in Ontario to a person outside of Ontario if:

- the individual consents to the disclosure,
- *PHIPA* permits the disclosure,

Can a custodian store, access or disclose personal health information outside of Ontario?

- the person receiving the information performs functions comparable to the functions of certain persons to whom the disclosure in Ontario is permitted,
- the custodian is a prescribed entity and the disclosure is for the purpose of health planning or health administration, the information relates to health care provided in Ontario to a person who is a resident of another province or territory of Canada and the disclosure is made to the government of that province or territory,
- the disclosure is reasonably necessary for the provision of health care to the individual and the individual has not expressly instructed the custodian not to make the disclosure or
- the disclosure is reasonably necessary for the administration of payments in connection with the provision of health care to the individual or for contractual or legal requirements in that connection.

FUNDRAISING AND MARKETING

CAN CUSTODIANS COLLECT, USE OR DISCLOSE PERSONAL HEALTH INFORMATION FOR FUNDRAISING ACTIVITIES?

The regulations contain specific requirements and restrictions that apply to all collections, uses and disclosures of personal health information for fundraising, including the following:

- The collection, use or disclosure of personal health information for fundraising purposes is only permitted where the fundraising relates to a charitable or philanthropic purpose related to the custodian's operations.
- All solicitations must contain an easy opt-out from any further solicitations.
- No solicitations may contain information about an individual's health care or state of health.

In general, custodians are only permitted to collect, use or disclose personal health information for purposes that are not related to the provision of health care with the express consent of the individual in question. However, *PHIPA* and its regulations provide that a collection, use or disclosure of an individual's name and mailing address (or the name and mailing address of a substitute decision-maker, if applicable) for fundraising may take place with the implied consent of the individual in question, as long as the following requirements are met:

- at the time the service has been provided to the individual, the custodian has posted, or has made available to the individual, a notice informing the individual of the custodian's intention to use or disclose the information for fundraising purposes, along with information on how the individual can easily opt out and
- the individual had not opted out within 60 days from the time the notice had been provided.

For personal health information collected before November 1, 2004, a custodian may assume implied consent to use or disclose an individual's name and contact information for fundraising, unless the custodian is aware that the individual has expressly withheld or withdrawn consent.

For further information please see the IPC fact sheet, *Fundraising under PHIPA*.

CAN PERSONAL HEALTH INFORMATION BE COLLECTED, USED OR DISCLOSED FOR MARKETING PURPOSES?

A custodian can only collect, use or disclose personal health information about an individual for market research or for marketing purposes with the express consent of the individual.

Note that the following activities are excluded from the definition of marketing:

- communications by health care practitioners about the availability of non-OHIP covered charges for a block fee or on the basis of a set fee for service and
- communications by Canadian Blood Services for recruiting donors of blood and blood products.

RESEARCH

WHAT ARE THE REQUIREMENTS FOR THE COLLECTION, USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION FOR RESEARCH?

The general rule is that a custodian needs to obtain an individual's consent to collect, use and disclose personal health information, unless *PHIPA* allows the collection, use or disclosure without consent. In recognizing the importance of health research, *PHIPA* permits the collection, use or disclosure of personal health information for research purposes without an individual's consent, if strict conditions are met.

For example, a custodian who uses personal health information for research and, similarly, a researcher who seeks disclosure of personal health information for research purposes, must both submit a detailed research plan to a Research Ethics Board (REB) for approval. When deciding whether to approve a research plan involving the use or disclosure of personal health information without consent, a REB must consider:

- whether the research can be reasonably accomplished without using the personal health information,
- the public interest in conducting the research and in protecting privacy,
- whether obtaining consent is impractical and
- whether adequate safeguards will be in place to protect the privacy of individuals and the confidentiality of their personal health information.

A researcher requesting disclosure of personal health information from a custodian must submit to the custodian a written application, a research plan and a copy of the decision approving the research plan by a REB. In addition, the custodian must enter into an agreement with the researcher that may impose further restrictions, including the manner in which the researcher may use and disclose the personal health information.

A researcher with an approved research plan who receives personal health information from a custodian shall:

- comply with the conditions, if any, imposed by the REB,

What are the requirements for the collection, use and disclosure of personal health information for research?

- use personal health information only for the purpose set out in the research plan,
- not publish information in a form that could reasonably enable a person to identify the individual,
- not disclose information unless required by law or if the disclosure is to prescribed persons or registries,
- not attempt to contact the individual whose personal information is the subject of the research project unless the custodian obtains the consent of that individual,
- notify the custodian in writing of any breaches of either the agreement or *PHIPA* and
- comply with the agreement between the researcher and the custodian.

Researchers are permitted to disclose personal health information to another researcher or to a prescribed person or a prescribed entity if the disclosure is either part of a research plan approved by a REB, or it is necessary for the purpose of verifying or validating the information or the research.

ARE THERE ANY REQUIREMENTS FOR RESEARCH ETHICS BOARDS AND RESEARCH PLANS?

Yes. The regulations specify that a REB must have at least five members, including:

- a member who has no affiliation to the person who established the REB,
- a member who has knowledge in privacy issues,
- a member who has knowledge in research ethics and
- at least two members with expertise in the methods or the relevant areas of research.

In addition, the regulations list a number of requirements that research plans must include. For example, a research plan must include a description of why consent to the disclosure of personal health information is not being sought from the individual to whom the information relates; a description of how the information will be used, the safeguards the researcher will put in place to protect the confidentiality and security of the information and a description of all persons who will have access to the information.

ONTARIO HEALTH CARDS AND HEALTH NUMBERS

WHO CAN COLLECT, USE OR DISCLOSE ONTARIO HEALTH NUMBERS AND UNDER WHAT CIRCUMSTANCES?

Custodians and certain persons or organizations prescribed in the regulations are permitted to collect, use or disclose Ontario health numbers.

A person or organization that is not a custodian or an agent of a custodian may only collect or use an Ontario health number for the following purposes:

- for purposes related to the provision of provincially funded health resources,
- for the purposes for which the custodian disclosed the number,
- for purposes related to the duties or powers of a governing body of health care practitioners who provide provincially funded health resources or
- for health administration, health planning or health research or epidemiological studies by persons listed in the regulations including, the WSIB, prescribed persons and prescribed entities.

An organization or person who is not a custodian or agent of a custodian may not disclose a health number, except as set out in the regulations or as required by law.

These restrictions on the collection, use and disclosure of health numbers do not apply to:

- a person who collects, uses or discloses health numbers for a proceeding,
- a prescribed entity or
- the individual or the individual's substitute decision-maker.

ARE OTHER ORGANIZATIONS PERMITTED TO REQUEST THE PRODUCTION OF A HEALTH CARD?

PHIPA states that only a person who provides a provincially funded health care resource may require the production of an individual's health card.

Are other organizations permitted to request the production of a health card?

However, there is nothing in *PHIPA* that prevents an organization from requesting a health card, as long as it is made clear that disclosure is voluntary and the information will only be used for purposes directly related to the provision of provincially funded health resources. For instance, an employer may allow an employee to voluntarily provide a health card in order to expedite the provision of health care services in the event of an emergency. A school, day care, or camp may also request a child's health number so that it is on record in the event of a medical emergency.

Please note that any such disclosure must be voluntary, and non-custodians may not require the production of health cards. It is an offence under *PHIPA* for any organization to wilfully collect, use or disclose any personal health information—including health numbers—in a manner that contravenes *PHIPA*.

An organization, for example a private sector business not directly involved in the delivery of provincially funded health services, is not permitted to take note of, record, collect, or use a health number for identification purposes. However, nothing prevents individuals from voluntarily choosing to show their health cards in order to verify identity. For example, individuals may voluntarily decide to provide their health cards to librarians in order to confirm their identity and obtain a library card. The librarians may view the health card, but are not permitted to record the health number.

For further information, please see the IPC document, *Frequently Asked Questions: Health Cards and Health Numbers*.

ACCESS TO RECORDS OF PERSONAL HEALTH INFORMATION AND CORRECTION

ACCESS

ARE INDIVIDUALS PERMITTED TO ACCESS THEIR OWN PERSONAL HEALTH INFORMATION?

With limited exceptions, *PHIPA* provides individuals with a general right to access their personal health information held by a custodian and sets out a formal procedure for access requests. The right of access does not apply to:

- records that contain quality of care information,
- personal health information required for quality assurance programs,
- raw data from psychological tests or assessments,
- personal health information used solely for research purposes or
- personal health information that is in the custody or under the control of a laboratory in respect of a test, where an individual has the right of access to that information from the health care practitioner and the practitioner has not directed the laboratory to provide the information directly to the individual.

As previously noted, personal health information includes identifying information that is not personal health information, but that is contained in a record that contains personal health information. Personal health information does not include identifying information if the information relates primarily to one or more employees or other agents of the custodian and the record is maintained primarily for a purpose other than the provision or assisting in the provision of health care.

For further information please see the IPC fact sheet, *Your health information: Your access and correction rights*.

HOW DO AN INDIVIDUAL OBTAIN ACCESS TO THEIR PERSONAL HEALTH INFORMATION?

An individual may exercise a right of access to a record of personal health information by making a written request for access to the custodian that has custody or control of the information.

The custodian should then either make the record available for examination or provide a copy of the record. Otherwise, the custodian must give a written notice to the individual seeking access stating that, after a reasonable search, the record does not exist, cannot be found or is not a record to which access applies. If the custodian is entitled to refuse the request, in whole or in part, the custodian must give a written notice stating that the request is being refused and providing reasons for the refusal. The notice must also state that the individual is entitled to make a complaint about the refusal to the IPC. If an individual decides to complain to the IPC, the complaint must be in writing.

The request must contain sufficient detail to allow the custodian to locate the record in question. Where the individual has not provided sufficient detail to enable the custodian to identify and locate the record, the custodian is required to assist the individual in reformulating the request.

Nothing in *PHIPA* prevents a custodian from granting an individual access to a record of personal health information if the individual makes an oral request for access.

For further information, please see the IPC's *PHIPA Practice Directions, Clarifying Access Requests and Drafting a Letter Responding to a Request for Access to Personal Health Information*.

HOW LONG DOES A CUSTODIAN HAVE TO RESPOND TO AN INDIVIDUAL'S REQUEST FOR ACCESS TO PERSONAL HEALTH INFORMATION?

A custodian must respond no later than 30 calendar days after the request was made.

Extensions of up to a maximum of 30 additional calendar days are allowed, where meeting this time frame would unreasonably interfere with the custodian's operations, or where the necessary consultations would not make it reasonably practical to reply within that time frame. In such situations, the custodian must inform the individual in writing of the extension and set out the length of the extension and the reasons for the extension.

CAN A CUSTODIAN REFUSE TO PROVIDE ACCESS TO AN INDIVIDUAL'S PERSONAL HEALTH INFORMATION?

Generally, custodians are responsible for providing individuals with access to their records of personal health information.

Custodians may only refuse access in limited situations, including:

- the information in question is subject to a legal privilege,
- access could reasonably be expected to result in a risk of serious harm to the treatment or recovery of the individual or serious bodily harm to the individual or another person,
- the information was collected in the course of an inspection, investigation or similar procedure and the resulting proceedings, appeals or processes have not yet been concluded or
- another law prohibits the disclosure of that information.

If an exception applies, an individual still has a right of access to the part of the record that can reasonably be severed from the part containing the information to which the individual does not have the right of access. If a custodian denies an individual access to the personal health information, the individual has the right to file a written complaint with the IPC.

IS THERE A FEE ASSOCIATED WITH AN ACCESS REQUEST?

Custodians may charge a reasonable fee for providing access to an individual's records of personal health information. *PHIPA* also permits a custodian to waive all or part of the fee associated with an access request. In charging a fee, *PHIPA* requires custodians to first provide the individual with a fee estimate. The fee amount must not exceed the prescribed amount set out in the regulations, if any, or the amount of reasonable cost recovery.

There is currently no regulation prescribing the fee for providing access to an individual's records of personal health information. Order HO-009 found that a custodian may charge a set fee of \$30 for photocopying or printing the first 20 pages of a record and 25 cents per page for every additional page. The set fee of \$30 also includes additional activities, for example, locating and retrieving the record, reviewing the contents of the record for not more than 15 minutes and preparing a response letter to the individual.

WHAT IF THE CUSTODIAN WORKS FOR A NON-CUSTODIAN THAT IS COVERED UNDER PUBLIC SECTOR ACCESS AND PRIVACY LEGISLATION, SUCH AS A SCHOOL BOARD OR MUNICIPALITY?

The provisions of *PHIPA* regarding access to, and correction of, personal health information do not apply to records in the custody or under the control of a health care practitioner who is employed by or acting for an institution within the meaning of the *Freedom of Information and Protection of Privacy Act*, which covers provincial ministries and most provincial boards, agencies and commissions, or the *Municipal Freedom of Information and Protection of Privacy Act*, which covers local government organizations such as municipalities, police, school, health and library boards, if the individual has the right to request access under either of those Acts. In that case, the individual would submit an access request under *FIPPA* or *MFIPPA*, as applicable. For example, if an individual wants to access personal health information compiled by a psychologist who works for a school board, the individual should make the request to the freedom of information coordinator of the custodian's institution, for example the school board, in accordance with *MFIPPA*, rather than directly to the custodian.

If the custodian works for a non-custodian that is not covered under *FIPPA* or *MFIPPA*, for example a private sector organization, the provisions of *PHIPA* would apply. In that case, the individual would submit an access request under *PHIPA* directly to the custodian.

CORRECTION

CAN INDIVIDUALS CORRECT ERRORS IN THEIR PERSONAL HEALTH INFORMATION?

An individual who believes that personal health information is incomplete or inaccurate may request that a custodian correct the record. It is the responsibility of the custodian to ensure that personal health information is complete and accurate.

For further information please see the IPC fact sheet, *Your health information: Your access and correction rights*.

HOW DOES AN INDIVIDUAL CORRECT ERRORS?

An individual seeking a correction to personal health information may submit a request to the custodian who has custody or control of the records. The custodian is permitted to make a correction based on an oral request; however, the custodian may require that the request be made in writing.

The custodian must respond within 30 days of receiving a written correction request. *PHIPA* provides limited grounds for extending this 30-day time frame. Extensions of up to a maximum of 30 additional days are allowed, where replying within 30 days would unreasonably interfere with the custodian's operations, or where the necessary consultations would not make it reasonably practical to reply within that time frame. In such situations, the custodian must inform the individual in writing of the extension and set out the length of the extension and the reasons for the extension.

CAN A CUSTODIAN REFUSE TO CORRECT AN INDIVIDUAL'S PERSONAL HEALTH INFORMATION?

Subject to the exceptions set out in the next paragraph, a custodian is obligated to correct a record of personal health information where an individual demonstrates, to the satisfaction of the custodian, that the record is inaccurate or incomplete for the purposes for which the custodian uses the information and the individual gives the custodian the necessary information to correct the record.

However, a custodian may refuse to correct a record of personal health information that was not originally created by the custodian and which the custodian does not have sufficient knowledge, expertise and authority to correct, or if the record consists of a professional opinion or an observation that a custodian has made in good faith, for example, a medical diagnosis made by a physician. If a correction is refused, the custodian is required to inform the individual of the refusal, the reasons for the refusal, the individual's right to file a complaint regarding the refusal to the IPC and the right of the individual to attach a statement of disagreement to the record.

ADMINISTRATION AND ENFORCEMENT

HOW IS *PHIPA* ENFORCED?

The IPC has been designated as the independent oversight body responsible for ensuring that custodians collect, use and disclose personal health information according to the rules set out in *PHIPA*. The IPC plays a significant role in enforcing overall compliance.

The IPC has various powers under *PHIPA*, including the authority to review and adjudicate complaints. These include the authority to:

- require a complainant to try to resolve the issue directly with the custodian,
- appoint a mediator to resolve the complaint and/or
- review a complaint initiated by an individual or, in the absence of a complaint, self-initiate a review where there are reasonable grounds to do so.

The IPC also has the authority to issue orders requiring compliance with *PHIPA*. For example, the IPC may order a custodian to:

- provide the individual with access to a record of personal health information,
- correct a record of personal health information,
- dispose of records of personal health information and
- change or cease a particular information practice.

HOW DOES AN INDIVIDUAL INITIATE A COMPLAINT?

A person who believes that another person has contravened, or is about to contravene *PHIPA*, has the right to submit a written complaint to the IPC. For example, a person may complain about:

- a custodian's information practices,
- a refusal to grant access to personal health information or
- a refusal to correct or amend personal health information.

For further information please see the IPC document, *Access and Correction Complaints – Personal Health Information Protection Act*.

How does an individual initiate a complaint?

IS THERE A TIME LIMIT WITHIN WHICH AN INDIVIDUAL MAY COMPLAIN?

In general, an individual must file a complaint with the IPC within one year from when the individual became aware of the problem. The legislation provides the IPC with the discretion to extend this one year limitation period.

For complaints that deal with access or correction, an individual must file a complaint with the IPC within six months from the time a custodian refuses an access or correction request.

IF A PERSON IS NOT SATISFIED WITH AN IPC ORDER, WHAT CAN BE DONE?

Persons affected by most types of orders issued by the IPC have the right to appeal on a question of law to the Divisional Court of Ontario within 30 days of receiving a copy of the order. Where the IPC issues an order relating to access or correction of health records, there is no right of appeal. In such a case, a person may apply to the Divisional Court of Ontario for judicial review.

CAN A PERSON SEEK COMPENSATION FOR DAMAGES?

A person affected by an order of the IPC or a person affected by conduct leading to a conviction for an offence under *PHIPA*, that has become final, may commence a proceeding in court for damages for actual harm suffered. If a court determines that the harm suffered was caused by wilful or reckless misconduct, *PHIPA* permits the court to award up to \$10,000 in damages for mental anguish.

WHAT IS AN OFFENCE UNDER *PHIPA*?

Offences under *PHIPA* include:

- wilfully collecting, using or disclosing personal health information in contravention of *PHIPA* or its regulations,

- requesting access to or correction of a record of personal health information under false pretences,
- intentionally disposing of a record of personal health information to avoid providing access,
- collecting, using or disclosing an individual's health number in contravention of *PHIPA*,
- obstructing the IPC, or one of its delegates, in the performance of its oversight functions,
- dismissing, suspending, demoting, disciplining, harassing or disadvantaging an individual who has alerted the IPC of an alleged contravention of *PHIPA* or
- failing to comply with an IPC order.

WHAT ARE THE CONSEQUENCES FOR COMMITTING AN OFFENCE UNDER *PHIPA*?

A natural person found guilty of committing an offence under *PHIPA* can be liable for a fine of up to \$50,000. A person who is not a natural person for example, an organization or institution can be liable for a fine of up to \$250,000.

Any officer, member, employee or agent of a corporation found to have authorized or acquiesced to a breach of *PHIPA* can be held personally liable.

In addition, persons who are convicted of an offence under *PHIPA* may be subject to a civil suit for damages for breach of privacy. Generally, custodians who have acted reasonably and in good faith will be protected from liability.

WHO IS RESPONSIBLE FOR PROSECUTING OFFENCES UNDER *PHIPA*?

No person other than the Attorney General, or an agent for the Attorney General, may commence a prosecution for an offence under *PHIPA*. A proceeding to prosecute an offence cannot be commenced after six months from the time the offence under *PHIPA* was alleged to have been committed.

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three Acts, the Commissioner:

- Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction;
- Investigates complaints with respect to personal information held by government or health care practitioners and organizations;
- Conducts research into access and privacy issues;
- Comments on proposed government legislation and programs; and
- Educates the public about Ontario's access and privacy laws.



**Information and Privacy
Commissioner of Ontario**

**Commissaire à l'information et à la
protection de la vie privée de l'Ontario**

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

September 2015