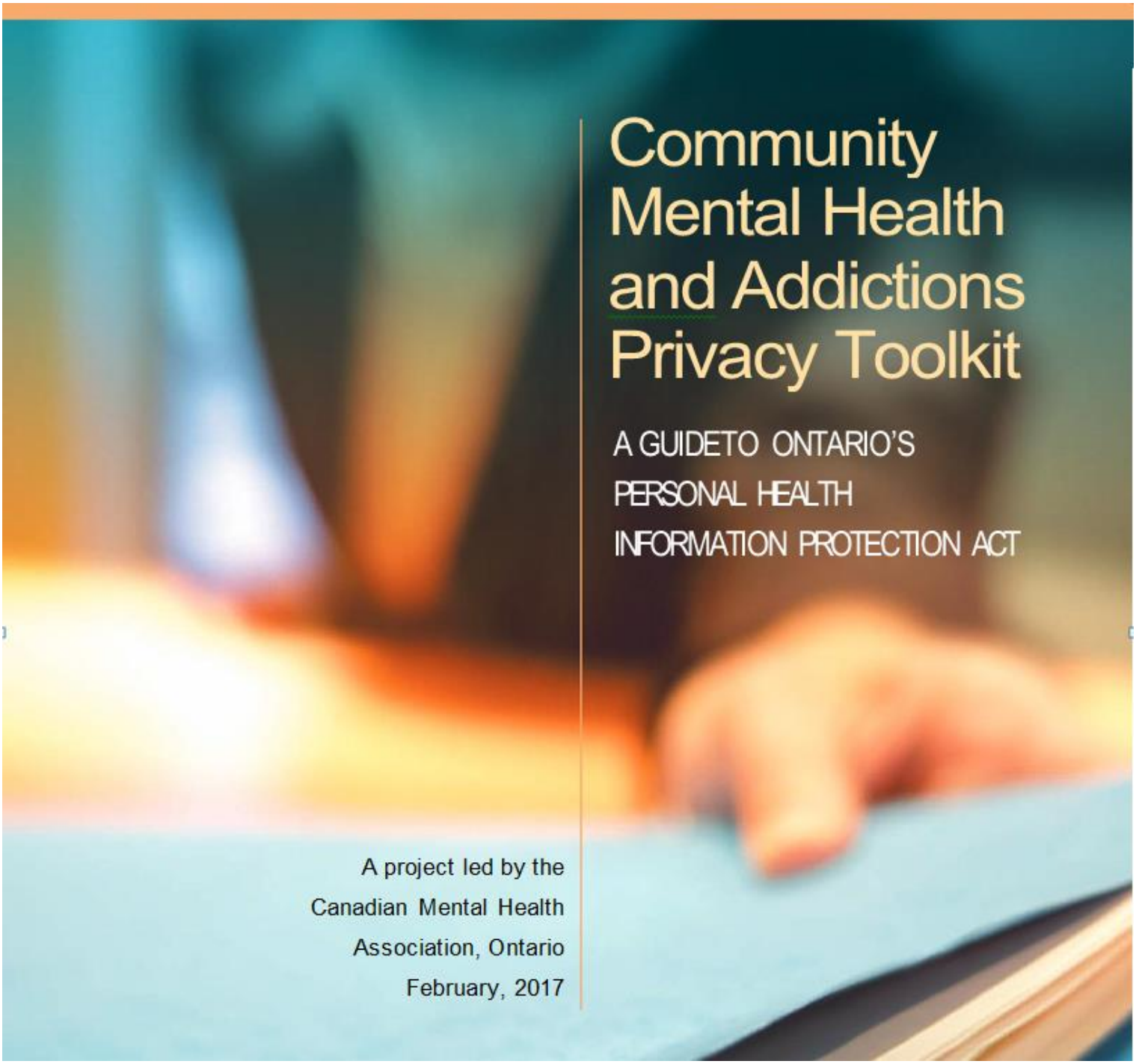

Community Mental Health and Addictions Privacy Toolkit
A GUIDE TO ONTARIO'S PERSONAL HEALTH INFORMATION PROTECTION ACT
A project led by the Canadian Mental Health Association, Ontario
February, 2017

Disclaimer

The material in this Toolkit is intended to assist community mental health and community addictions stakeholders to understand their obligations under the *Personal Health Information Protection Act, 2004* (PHIPA). By its nature it provides information, but is not a complete review of the law. It is current to January 31, 2017.

It is for general reference, and directs you to other more complete sources of information about PHIPA, including the Act itself. It does not cover every possible scenario you may encounter.

The Toolkit should not be relied on as legal advice or professional opinion. If you have specific questions about its content or the Act, you should consult a lawyer.

Another helpful resource is the Office of the Information and Privacy Commissioner of Ontario, which provides general guidance on how the Act applies. Helpful materials are available online at: www.ipc.on.ca:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Tel: (416) 326-3333 Toll-free: 1-800-387-0073

You may wish to adapt the tools, checklists and templates in this Toolkit to fit your particular circumstances. Companion policies were kindly provided directly by CMHA Waterloo Wellington.

All references to “clients” in the Toolkit should be read to mean “individuals,” “patients,” “consumers” and “customers,” as appropriate. Where the context requires it (i.e., upon a legal finding of incapacity) “client” includes the client’s substitute decision-maker.

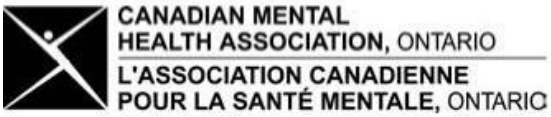
Table of Contents

Acknowledgements

The 2017 Toolkit amendments presented here were authored at the invitation of CMHA Ontario by Mary Jane Dykeman (DDO Health Law), with Anna Tersigni Phelan (CMHA Waterloo Wellington).

This Toolkit was first published in September 2005. Its principal author was Mary Jane Dykeman, consultant to CMHA Ontario, in association with then CMHA Ontario staff, Ministry of Health and Long-Term Care staff and an advisory group of community mental health and addictions representatives:

Mary Jane Dykeman
Linda Marmen
Karen McGrath
Scott Mitchell
Liz Scanlon
Glenn Thompson
Halyna Perun
Michele Sanborn
Ruth Stoddart
Brenda Bunting
Diana Capponi
Greg Howse
Harry Spindel
Jeff Wilbee
Victor Willis
Brigitte Witkowski
Josh McLennan Design



CHAPTER 1

This chapter will help you understand how PHIPA applies to you. It provides general background, including important definitions. It also describes what kind of information PHIPA does and does not cover.

Complying with the Personal Health Information Protection Act (PHIPA)

KEY POINTS

PHIPA came into force on November 1, 2004. Since then, PHIPA has been amended several times over the years, and most recently, Bill 119 received Royal Assent on May 18, 2016. These most recent changes amended PHIPA with a focus on protecting patient privacy and providing the framework for the development and maintenance of electronic health records in Ontario.

You need to be familiar with various terms and concepts in order to know what your responsibilities are under the Act. These include “personal health information” (PHI), “health information custodian,” “agent” of a custodian, “recipients” of PHI, “health care,” “collection,” “use” and “disclosure.” (These and other terms are listed in the Glossary at the end of the Toolkit.)

One of the most important considerations is whether you are (or your organization is) a health information custodian, an agent of a custodian or a recipient of PHI. This will depend on your primary function, and whether it is to provide “health care” as defined in PHIPA.

You must also understand when PHIPA will not apply to you.

Background and key definitions

PHIPA became law on November 1, 2004, and as amended by Bill 119 does a number of things:

- It creates a common set of rules for the collection, use and disclosure of personal health information (PHI) for use by “health information custodians” (also called “custodians”).
- It requires certain practices to be in place to protect PHI.
- It describes the circumstances in which you can share PHI within your agency, and circumstances in which you can or must give it to someone outside your agency.
- It provides rules for consent, capacity and substitute decision-making in relation to PHI.
- It promotes the appropriate sharing of PHI so that clients can receive and benefit from integrated health services.
- It creates rules for access to and correction of records of PHI.
- It provides rules for notifying the Information and Privacy Commissioner of Ontario and individuals whose PHI that is in the custody of custodians in the event of a theft, loss or unauthorized use or disclosure,
- It sets out fines for the persons guilty of offences under PHIPA (with no limitation periods).
- It sets out rules for the collection, use and disclosure of electronic health records. At the time of publishing this version of the Toolkit, Part V.I of PHIPA had not yet been proclaimed into force.
- It designates the Information and Privacy Commissioner of Ontario as the body that oversees compliance with the Act.

Personal Health Information (PHI)

PHI can be oral (spoken) or recorded (written on paper or electronically). To help you determine whether information you have is defined as PHI, you should ask yourself the following questions:

- Is it information that on its own, or if it's reasonably foreseeable in the circumstances, will be linked to other information, can be used to identify an individual?
- Does it relate to the physical or mental health of the individual, including his/her family history?
- Does it relate to the health care an individual has received, or identify the people responsible for providing health care to that individual?
- Is the information an individual's plan of service within the meaning of the Home Care and Community Services Act, 1994? A plan of service under that Act refers to certain types of services that are provided in the community and coordinated through designated agencies. They include such things as meals, caregiver support and personal assistance services. This is different than a plan of treatment described in the Health Care Consent Act and Mental Health Act.
- Does it relate to the individual's payment or eligibility for health care or for eligibility for coverage for health care (including eligibility for coverage under the Ontario Health Insurance Plan [OHIP])?
- Does it relate in any way to the individual's donation of body parts or bodily substances (including their testing)?
- Is it the individual's health (OHIP) number?
- Does it tell you who the individual's substitute decision-maker is?
- Is it part of a record that contains PHI, even if it is not itself PHI? (This is called a "mixed" record, which is covered as PHI under the Act.)

If you have answered "Yes" to any of these questions, the information is PHI.

QUESTIONS AND ANSWERS

Q. Our case management programs provide services to clients in the community. We meet clients in public places (such as libraries and coffee shops) and it is possible that other members of the community may recognize us as health care professionals and conclude that the client is under our care. This could have a negative impact on the client. Does PHIPA prevent or place restrictions on this practice?

A. Technically, identifying a health care provider as giving care to the individual is PHI under the Act. You may want to notify the patient of the risks associated with meeting them in public places (such as of being overheard despite your best efforts to have a discreet conversation; or of someone recognizing both of you and presuming that this person is your client). You could include this in your written public statement, or state the risks verbally as part of your intake process with clients. This is a choice that the client may make, just as he or she could be seen by others entering your building. But it will be important to have that conversation with the client about privacy.

Are you a health information custodian or an agent?

Health information custodians

PHIPA applies primarily to "health information custodians" (custodians) who are named under the Act. These include a person who operates

- a public hospital,
- a psychiatric facility,
- a long-term care home, or
- a laboratory.

In these examples, the "person who operates" is typically a Board of Directors or other group with corporate responsibility for the organization.

Other custodians include

- health care practitioners, whether they are regulated (such as occupational therapists and nurses) or unregulated (such as mental health counsellors, as long as they are providing health care for payment), and
- the Minister of Health and Long-Term Care, together with the Ministry, as they are responsible for planning and funding Ontario's health services and, as a result, hold PHI.

A person who operates the following is also included in the definition of custodian:

- a centre, program or service for community health or mental health whose primary purpose is the provision of health care.

This means that mental health and addictions agencies, programs and services that provide health care directly to clients are custodians and need to be aware of the rules under PHIPA.

Is your primary purpose to provide health care?

If you still have questions about whether you are a custodian, consider PHIPA's definition of "health care." Health care is any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and is carried out or provided

- to diagnose, treat or maintain an individual's physical or mental condition,
- to prevent disease or injury or to promote health, or
- as part of palliative care.

This includes

- making, dispensing or selling drugs, devices and equipment or other items by prescription, or
- community services provided under the Home Care and Community Services Act, 1994 (discussed above).

If any of the items in the list above describe your main function, you are a custodian and have all of the responsibilities of a custodian under PHIPA. There are a few exceptions, including the following:

- If you are the "agent" of a custodian (see below)
- If you are an aboriginal healer who provides aboriginal healing services to aboriginal persons or members of the aboriginal community
- If you treat another person solely by prayer or spiritual means based on your religion
- If you are acting on behalf of a person who is not a custodian, and the main purpose of your work is not health care

Are you an agent of a custodian?

PHIPA also applies to a custodian's "agents" if they collect, use, disclose, retain or dispose of PHI on behalf of the custodian. These include

- employees and consultants,
- health-care practitioners (if they are acting on behalf of the custodian),
- volunteers,
- researchers,

- students, and
- independent contractors (including physicians and third-party vendors who provide you with supplies or services).

For example, a staff member of an addictions program is an agent of the program under PHIPA. So is the shredding company you hire to dispose of files that contain client PHI. Agents must

- collect, use, disclose, retain or dispose of PHI with the same care and diligence as the custodian (given that agents collect, use, disclose, retain or dispose of PHI on behalf of the custodian, and not for their own purposes),
- comply with the custodian's obligation to collect as little PHI as needed in the circumstances, and not collect PHI if other information would suit the purpose,
- collect, use, disclose, retain or dispose of PHI as necessary in the course of their duties,
- not collect, use or disclose it when other information is available,
- protect it from being lost, stolen or inappropriately accessed, as well as from unauthorized copying, modification and disposal, and
- comply with any conditions or restrictions that a HIC would impose on the agent
- tell the custodian as soon as possible if the PHI that the agent possesses or handles on behalf of the custodian is lost or stolen, or if someone accesses it without authority.

Custodians should reinforce these expectations with all of their agents. This can be done in a variety of ways:

- Providing education on PHIPA (in person, and through notice boards, publications and other written materials)
- Reinforcing a privacy culture throughout your agency, and being clear about your expectations
- Building a privacy component into annual performance reviews
- Reviewing existing contracts with third party vendors to ensure that they have adequate safeguards for PHI

QUESTIONS AND ANSWERS

Q Where do “non-traditional” mental health and addictions service providers such as consumer and family initiatives fit under PHIPA?

A These providers are not custodians under PHIPA (unless they are agents of a custodian who collect, use or disclose PHI for the custodian’s purpose and not their own – such as where a peer counsellor is employed by a mental health or addictions agency, or is acting as a volunteer for the agency).

Q What about alternative work programs?

A It may depend. Consumer or family initiatives and alternative work programs would have to say “Yes” to all of the following criteria in order to be custodians:

- They are a program or service for community health (including addictions) or community mental health.
- They collect, use and disclose PHI.
- Their primary purpose is providing health care.

Typically, the primary purpose of these groups is not health care under the definition of PHIPA. Instead, their primary purpose might be to support, educate and advocate on behalf of consumers or families. Or, in the case of an alternative work program, its main purpose is likely to provide job opportunities for those suffering from a mental illness; its main purpose is employment, and not health care.

Even if they are not agents of a custodian and do not fit squarely under PHIPA, these organizations could still model their privacy and information practices on the Act. The only difference would be that there would be fewer formal rights and obligations (for example, clients would not have the right to make a complaint to the Information and Privacy Commissioner).

Q Where do housing providers fit under PHIPA?

A There are several types of housing providers to consider. Some fall under the definition of “health information custodian,” while others do not.

For example, if the relationship between the client and the housing provider is strictly one of a private landlord and tenant, under the *Residential Tenancies Act*, with a primary purpose of housing, the landlord is not a custodian under PHIPA. Express consent should be sought before any PHI is given to the landlord.

If a mental health agency provides housing as one of its services and acts as the landlord to its clients, there is no problem in sharing the client’s PHI with the part of the agency that is arranging the housing, since both the person giving and receiving the PHI are agents of the custodian under

the Act. PHI can be shared in this way based on the client's implied consent, if you wish to do so. You are also free to ask for the client's express consent, if that is your preferred approach.

However, if the mental health agency leases housing units from a private landlord for the agency's clients, PHI should only be provided to the landlord with the individual's consent. For example, it could be clear to a landlord that a new tenant is a client of a mental health agency. Technically, this is a disclosure of PHI. The landlord is not a custodian under PHIPA, and express consent of the client is required.

A person who operates one of the following types of homes is named as a custodian under PHIPA (note that this is not the full list):

- A home for special care under the Homes for Special Care Act
- A retirement home under the Residential Tenancies Act, 2006

When does PHIPA not apply?

PHI in employment files

PHIPA applies to your employee's records of PHI only if they are kept mainly for the purpose of providing health care or assisting in providing health care. For example, if your employee's file has a doctor's note in it that explains an employee's absence from work, that PHI is not covered under the Act, as the record is kept primarily for employment purposes, not primarily for health care purposes.

However, if an employee becomes a client of your agency, the record you keep about the care you provide to that employee would be covered under PHIPA.

What has been open to recent debate is the issue of records that a custodian has about the custodian's employees that are kept for occupational health and safety reasons. For example, if the agency, as an employer, brings in a nurse to provide flu shots to all staff, the information in the nurse's hands is PHI; the nurse brought in from the outside is providing a health care service. Once the information is disclosed (with the client's consent) to the agency to be placed in a file to show compliance with the Occupational Health and Safety Act, it is not being kept for a health care purpose and is therefore not PHI.

Recipients

Generally, anyone who holds PHI outside the health sector is not covered under PHIPA (such as insurance companies, employers, school boards and others). Only a few specific rules under PHIPA are important for these types of third parties (called "recipients") who obtain PHI from a custodian. For example, if a client gives an addictions program consent to release PHI to an insurance company, PHIPA places limits on how the insurance company can then use or disclose that information. However, it should be very clear that the client's express consent is required for a custodian to release information, unless some other legal authority exists.

Recipients are not agents of the custodian because they do not collect, use or disclose PHI on the custodian's behalf. Typically, a recipient's activities are very separate from the custodian's.

Examples of recipients include

- schools,
- insurance companies,
- employers,
- family members (unless they have legal authority to act on behalf of the client, such as acting as the client's substitute decision-maker), and
- courts or tribunals such as the Consent and Capacity Board.

In some cases, a custodian will be able to give information to a recipient without client consent, such as where PHIPA or another law allows or requires this disclosure.

Custodians are not “recipients,” even when they receive PHI from other custodians.

Other laws

You should follow the rules in PHIPA unless another law specifically says that it prevails over PHIPA. For example, the rules about community treatment orders in

the *Mental Health Act* prevail where they conflict with any of PHIPA’s rules.

It is best to stay current on any changes to the laws you rely on frequently. This is because when PHIPA came into force on November 1, 2004, it also made a number of changes to existing laws, including the Mental Health Act. Be aware that some situations may be governed by a law that takes priority over PHIPA, if there is a conflict between that law and PHIPA. The other laws may also give you additional discretion about how you may collect, use or disclose PHI.

For example, under subsection 35(2) of the *Mental Health Act*, an officer in charge of a psychiatric facility under that Act may now collect, use or disclose PHI about a patient, with or without the patient’s consent, for the purposes of examining, observing, assessing or detaining someone under the Mental Health Act; or to comply with the mental disorder provisions of the Criminal Code, including orders of a court or the Ontario Review Board. It will be up to these psychiatric facilities to decide when they will rely on this authority. These facilities will still have obligations under PHIPA, for example, to safeguard the PHI they hold and to provide clients with access to their records of PHI. This rule does not apply to community mental health agencies nor to addictions programs. However, the facility’s discretion to give PHI to you is worth noting.

For example, a court support worker employed by a mental health agency may need information from the psychiatric facility that performed a court-ordered assessment for a client. This section would give the officer in charge of the psychiatric facility the authority to disclose that information. Other sections of PHIPA that would apply (for example, where the facility may rely on the client’s implied consent to give you information) will be discussed further below.

QUESTIONS AND ANSWERS

Q A number of community service agencies and our local mental health facility (a psychiatric facility under the Mental Health Act) have created a database that contains client PHI. Information is accessible by each of the members of the database in order to support the client's integrated care and to reduce duplication of services. This is done with client consent.

Is the database a custodian under PHIPA? Instead of acting as separate custodians of the PHI in the database, could several service agencies act as one custodian?

A You should first look at the status under PHIPA of each of the community agencies and the mental health facility that will have access to the database:

- If each is a custodian under PHIPA, placing the information in a database is the same as giving it to another custodian under PHIPA.
- If someone who has access to the database is not a custodian (and is not the agent of a custodian), the information is shared with him/her as a third-party "recipient."

Getting a client's consent to give their PHI to the person who maintains the database is always a good idea, since it is not a use or disclosure a client might think you would typically make. You may be able to rely on implied consent, but it is important to remember that implied concept is a concept under PHIPA that only applies to information shared among custodians. If a non-custodian is part of the database, the information cannot flow based on implied consent. And a consent that is implied must be able, technically, to be withdrawn.

The database is not a custodian under PHIPA. However, the person who operates and maintains the database may be considered a "health information network provider" under the *Act*. For example, a provider that hosts data for two or more custodians in an electronic format, such as a database, is doing so for the purpose of allowing custodians to give PHI to each other. We are aware of some CMHAs acting in the role of health information network provider.

Special rules about health information network providers are provided in section 6 of the regulations to PHIPA, available online at: https://www.ontario.ca/laws/regulation/040329#BK7.

If your agency is involved in this type of arrangement with a health information network provider and other agencies, you should review this section very carefully; it sets out multiple requirements for those who supply electronic services to custodians, including health information network providers.

Some CMHAs have been asked by their local health integration network to take on the role of health information network provider. It is important to understand the obligations associated with that role, described in the link above. This includes a requirement to prepare both a privacy impact assessment and threat risk assessment. If you are a custodian providing personal health information to a health information network provider, make sure to ask for a copy of these documents, just as a matter of your own due diligence.

Two or more custodians may apply to the Ministry of Health and Long-Term Care to be named as a single custodian for the purpose of PHIPA. Doing so would cover them for all purposes of PHIPA, not just for the PHI in the shared database. See discussion of this issue in Chapter 2.

You can learn more about the single custodian application process online at: http://www.health.gov.on.ca/english/providers/project/priv_legislation/hic_application.pdf

Collection, use and disclosure

The concepts of collection, use and disclosure of PHI will be discussed in further detail in Chapters 4, 5 and 6 of this Toolkit.

CHAPTER 2

This chapter focuses on some basic responsibilities and other issues that custodians should be aware of under PHIPA.

Getting started: What health information custodians should know

KEY POINTS

If you are a custodian under PHIPA, you must take specific steps in order to comply with the Act, including

- naming a contact person,
- developing a public written statement about how you collect, use and disclose personal health information (PHI)
- putting in place appropriate security measures to protect PHI,
- keeping accurate records of PHI,
- meeting certain conditions if you keep records of PHI in a client's home
- taking steps to ensure that PHI is not collected without authority
- being responsible for your agents (those who collect, use, disclose, retain or dispose of PHI on your behalf),
- notifying an individual at first reasonable opportunity in the event of a theft, loss or unauthorized use or disclosure of PHI and include in the notice of statement that a complaint can be made to the Information and Privacy Commissioner,
- notifying the Information and Privacy Commissioner if the circumstances warrant it under the regulations,
- maintaining responsibility for your agent's even if PHI even if the collection, use, disclosure, retention or disposal of information was not carried out in accordance to PHIPA and
- ensuring that anyone who alerts the Information and Privacy Commissioner to a breach or possible breach of PHIPA is protected from harassment, demotion and other negative actions.

Custodians also need to be aware of

- the possibility of applying to the government to join together with one or more other custodians to act as a single custodian for the purposes of PHIPA (for example, to share their duties under the Act)
- the consequences of not complying with PHIPA, including the possibility of fines.

PHIPA REFERENCE

For more complete information, you should also look at the following sections of PHIPA: 3, 10-17, 70-72

Duties of a custodian

There are special rules under PHIPA that indicate what steps custodians must take in order to comply with the Act. These duties are described below.

Naming a contact person

You must appoint a “contact person” whose role is to help you meet your obligations under PHIPA. That person should

- take an active role in making sure you are complying with PHIPA,
- make sure your agents are informed about their duties under PHIPA,
- answer any questions and complaints that relate to your information practices, and
- respond to access and correction requests (unless someone else in your agency has that responsibility).

In most agency settings, the contact person is called the “privacy officer”.

QUESTIONS AND ANSWERS

Q I am a health care practitioner in private practice, but I occasionally consult with a community mental health agency. Do I need to name a contact person?

A When you are in your private practice, you have a choice: you can either name someone else as a contact person under PHIPA, or fulfill the duties yourself.

When you act on behalf of the community agency, the agency is the custodian and you are its agent. In that case, the agency is responsible for appointing someone as its contact person.

It is important to remember that in your private practice, as the custodian, you have all the duties described in this toolkit that other much larger custodians have (such as hospitals). This includes training your staff, volunteers, and anyone else who collects, uses, and discloses PHI on your behalf.

Developing a public written statement

You must develop a document such as a notice, fact sheet, brochure or poster that describes the purposes for which you collect, use and disclose PHI. You must include in it a general description of the administrative, technical and physical safeguards and practices that you maintain with respect to the PHI. This document must also inform people

- who your contact person is and how to get in touch with him/her,
- how a client can ask for access to (and correction of) the records of PHI you hold,
- how a client or member of the public can raise questions about your privacy practices or other matters relating to PHIPA, and
- how to complain to you, or about you to Ontario's Information and Privacy Commissioner.

Note: The goal is to be open about how you handle PHI. You can do this by taking steps that are reasonable under the circumstances to let people know how you will protect their individual privacy and the confidentiality of their PHI. This written statement must be made available to the public, and it is up to you to decide how to do that (for example, you could give clients a privacy notice, post information in your intake area and/or place information on your website).

A sample privacy notice is provided at the end of this chapter.

Protecting PHI with security safeguards

PHI must be protected. Although PHIPA does not tell you exactly what precautions you must take to keep the information secure, you must protect the PHI you hold, which could include the following types of safeguards:

- Administrative: by adopting policies and procedures that reinforce privacy protection
- Physical: by locking drawers and cabinets, and making sure that PHI to be disposed of is not placed in public or unsecured garbage bins
- Technical: by using password protection on computers, encrypting files and using secure servers

You must protect records of PHI against loss, theft or unauthorized

- collection
- access
- use
- disclosure
- copying
- modification
- disposal

If a privacy breach occurs in spite of your best efforts to protect the PHI you hold, you must notify your client and depending on the circumstances, the Information and Privacy Commissioner may be required to be notified as well. Based on the May 2016 amendments to PHIPA through enactment of Bill 119, the regulations to PHIPA will be amended to set out what kinds of breaches must be reported.

A template letter is provided at the end of this chapter for your reference. You should also consider whether it might be more appropriate to not send a letter, but to use the language in the template letter to inform your client about the situation at his/her next appointment,

- as long as the risk is low that he/she will not be contacted by a third party first,
- you are satisfied that the breach can be mitigated and no further harm is likely to come to the client, and
- if the appointment will take place in the near future.

The Information and Privacy Commissioner has posted some helpful information about how to safeguard the PHI you hold (including tips on its storage, retention, disposal, transfer, communication by email, audit), which can be found on the IPC website at: https://www.ipc.on.ca/:

- Safeguarding Personal Health Information, Fact Sheet # 1, January 2005,
- Secure Destruction of Personal Information (Dec 2005)
- Encrypting Personal Health Information on Mobile Devices (May 2007)
- Wireless Communication Technologies: Video Surveillance Systems (June 2007)
- Health-care requirement for strong encryption (July 2010)
- Secure Transfer of PHI (August 2012)
- Detecting and Deterring Unauthorized Access to Personal Information (January 2015)
- Communicating Personal Health Information by Email (September 2016)

Audits

A new standard was set as a result of a privacy breach at a community hospital where staff sold PHI to a registered education savings plan provider about new mothers and their babies. This resulted in numerous proceedings including a prosecution for securities fraud and a class action lawsuit. The Information and Privacy Commissioner of Ontario issued Order HO-013, which was subsequently appealed to Divisional Court and ultimately settled. This order, along with the Detecting and Deterring Unauthorized Access to Personal Health Information noted above, set a new standard for safeguarding PHI. If you are not conducting random audits on a regular basis, this is now considered best practice. In particular, check with your IT provider to ensure you meet the standards set out on pages 19-22 of Detecting and Deterring Unauthorized Access to Personal Health Information, which includes a framework for logging, monitoring and auditing collections, uses and disclosures of PHI in a systematic way.

Keeping accurate records

You must take reasonable steps to make sure that the PHI you hold is as accurate, complete and up to date as necessary for the purpose(s) for which you use it. If you are going to give PHI to someone else (outside your agency, for example), you need to tell that person or organization whether there are any limits to the PHI being accurate, complete or up-to-date for the purpose(s) that they require it.

QUESTIONS AND ANSWERS

Q My agency has pretty good record-keeping practices and my staff members take care to make sure our client files are accurate.

If a client asks me to disclose PHI to someone I don't know, how will I know whether the information is accurate for their purposes?

A You cannot possibly anticipate every situation where a client might ask you to give PHI to someone else. However, many requests involve releasing information to:

- other health care practitioners or organizations,
- employers, or
- lawyers.

If it is very obvious that something relevant is missing from the information that you are going to release, or that the record is otherwise incomplete or inaccurate, you may note that or identify that information is missing. Otherwise, you should make a note every time you disclose information that the PHI you are providing is up to date for your own purposes only. (Some custodians have dealt with this by stamping the document to be disclosed, or adding a cover letter to documents they disclose.)

Records in the home or elsewhere

If you want to keep records of PHI in the client's home or at other premises that you do not control, you can do so with the client's consent.

If you do, however, the records must be kept and protected in a reasonable manner. Before doing so, you must also abide by any relevant rules or restrictions of your professional college or other body that registers you to practice.

QUESTIONS AND ANSWERS

Q Our assignments require us to carry client PHI with us into the community. Does PHIPA prevent or place restrictions on this practice?

A The Act does not prevent you from carrying PHI into the community. However, it does state that a patient is to be notified if their record is lost, stolen or if it is use or disclosed without authority and in some cases if it meets the prescribed requirements, it must be reported to the Information and Privacy Commissioner. You should take every precaution with the record to ensure its safety. For example, don't leave the record on the seat of your car when you are not in the car.

There are special rules about leaving records of PHI in a client's home or other premises you don't control. You will need the client's consent, and should also consider what is reasonable in the circumstances. You may also be bound by any rules of your professional college, where they exist.

Agents

As discussed above, an agent is anyone who collects, uses, discloses, retains or dispose of PHI on your behalf (including staff or consultants, health care practitioners, researchers, volunteers, independent contractors and students).

As a custodian, you are responsible for your agents. Ultimately, you must take steps that are reasonable to ensure that your agents do not collect, use, disclose, retain or dispose of PHI contrary to PHIPA. You maintain this responsibility even if your agents act in an authorized way. You are also able to restrict, and impose any conditions or restrictions on your agents.

Agents can only act on your behalf if

- you are permitted or required to collect, use, disclose, retain or dispose of the PHI and only if necessary for the purpose of carrying out their duties as your agent,
- it is not contrary to the PHIPA or any other act,
- they comply with any conditions or restrictions that you may impose on them
- they comply with any prescribed requirements, if any.

Agents must:

- act within the scope of the custodian's authority (in other words, you cannot tell your agent to do something that you would not be allowed to do under PHIPA),
- notify you immediately if the PHI they hold on your behalf is stolen or lost, or if someone without proper authority accesses or has already accessed it, and

- comply with their legal reporting duties (such as to report child abuse under the Child and Family Services Act), even if the custodian has not specifically authorized the agent to do so, or has told the agent not to make the report.

General limiting principles

Under PHIPA, you should be careful to collect, use and disclose PHI

- only if it is specifically required (for example, if all you need is non-PHI, use it instead), and
- as judiciously and infrequently as possible. For example, staff should collect PHI only as necessary and when it is required from clients. Of course, you will want to ensure that all professional standards (and any policies of your agency) for documenting client information continue to be met.
- to ensure that it is not collected without authority

Protection for “whistleblowers”

No one is allowed to dismiss, suspend, demote, discipline, harass or disadvantage another person because that person has reported to the Information and Privacy Commissioner (who oversees compliance with the Act) about a past or future breach of the Act. This includes taking steps to stop the breach from occurring, or refusing to do something that would amount to a breach.

In other words, if someone genuinely thinks that you are not complying with the Act, PHIPA does not allow you to take punitive measures against that person because he/she has reported you to the Information and Privacy Commissioner.

Applying for single custodian status

Two or more custodians may apply to the Ministry of Health and Long-Term Care to be named as a single custodian for the purpose of PHIPA. However, under O.Reg 329/04, certain organizations are prescribed as single custodians. Doing so would cover them for all purposes of PHIPA, not just for a specific purpose such as responding to client requests to access information in a shared database (discussed above).

In this case, you will have to provide specific information, including but not limited to

- a description of why such an order would be in the public interest,
- how you would ensure that clients have reasonable access to their records of PHI,
- how single custodian status would allow you and the other custodians to provide integrated health care,
- how the order would affect your ability to comply with the Act, and
- any safeguards or other measures that you would put in place to ensure continued compliance with the Act.

Consequences of not complying with PHIPA

Being found guilty by Ontario's Information and Privacy Commissioner of an offence under PHIPA could result in fines of up to:

- $100,000 for individuals, or
- $500,000 for corporations.

These fines doubled in 2016. Most of the offences under PHIPA happen either if you knowingly, willfully or deliberately do something you know you should not do, or if you fail to do something that you should do. However, PHIPA protects you if you acted in good faith, so it could be important to show that you did.

In light of recent snooping cases, where employees who have access to patient medical records, such as snooping patient records containing PHI by employees, have found custodians liable for civil damages outside of PHIPA. Privacy breaches and your obligations will be further discussed in Chapter 11.

Once an offence has been proven, the person affected by your breach of the Act could also go to court to ask for compensation. This could include up to $10,000 for mental anguish, as well as general damages (a sum of money decided by the court).

Employees, agents, senior management and board members of community mental health agencies and community-based addictions programs should be aware of the possibility, however remote, that they could be personally liable under PHIPA. This could happen if they

- have authorized someone to commit an offence, or
- had the authority to prevent an offence but chose not to do so.

The overall message is not to frighten people about PHIPA, but to effectively secure the rights of all. You are protected under the Act if you act in good faith. However, it is always important to remember that you could someday be asked to prove that you acted in good faith, and that your privacy practices may be scrutinized.

Complying with the federal privacy legislation

A mental health or addictions program may be subject to both PHIPA and to the federal privacy legislation, the Personal Information Protection and Electronic Documents Act. The federal legislation applies if you collect, use or disclose personal information in the course of a commercial transaction. For example, if you run a parking lot or some type of retail store, act as a landlord or collect money in exchange for a service such as an education session, the federal legislation will apply if you collect personal information on a credit card or otherwise.

The federal legislation also applies to PHI. However, because PHIPA is likely to be designated by the federal government as being “substantially similar” to the federal legislation, you must follow the PHIPA rules.

TEMPLATES

TEMPLATE: PRIVACY NOTICE

Collection of Personal Health Information
We collect personal health information about you directly from you or from the person acting on your behalf. The personal health information that we collect may include, for example, your name, date of birth, address, health history, record of your visits to [name of agency] and the support you received during those visits.

Occasionally, we collect personal health information about you from other sources if we have obtained your consent to do so or if the law permits us to do so. We make sure that only those people who need to see your personal records are allowed to look at them. We protect your information through our administrative policies and by adopting appropriate safeguards and security measures.

Use and Disclosure of Personal Health Information
We may use or disclose your personal health information to

- communicate with your various health care providers including your family physician and/or other health care institutions for continuity of care, in order to treat/support and care for you (unless you tell us otherwise);
- plan, administer and manage our internal operations, and conduct risk-management activities;
- conduct quality improvement activities (such as sending client satisfaction surveys);
- teach, conduct research (only under strict rules overseen by a research ethics board) and compile statistics;

- support your care across multiple health care organizations via shared electronic health systems [Note: consider naming, or provide a link to somewhere on your site that explains which ones, e.g. Clinical Connect and similar systems]
- comply with legal and regulatory requirements;

and

- fulfill other purposes permitted or required by law.

We can assure you that only staff who need your personal health information for direct care, administrative purposes to assist in providing you care, or otherwise as permitted or required by law, are authorized to access your record of personal health information.

A client's instruction cannot prevent us from recording information that is required by law, professional standards or our practice.

To Access or Correct Your Information
If you believe a record of personal health information held by [name of agency] is inaccurate or incomplete, you may make a written request for correction. Please contact [name of contact person, name of agency, address, other contact information].

For More Information, Comments or Complaints

If you would like more information or have questions or concerns about our privacy and information practices, please contact: [name of contact person, name of agency, address, other contact information].

You may also make a complaint about our information and privacy practices to the Information and Privacy Commissioner at:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Tel: (416) 326-3333
Toll-free: 1-800-387-0073

[version number, date notice last amended/approved]

[YOUR LOGO HERE]

TEMPLATE: CONFIDENTIALITY AGREEMENT

I, _____, agree with the following statements:

I have read and understood [name of agency]'s Privacy Policy.

I understand that I may come in contact with confidential information during my time at [name of agency]. As part of the condition of my work with [name of agency] I hereby undertake to keep in strict confidence any information regarding any client, employee or business of [name of agency] or any other organization that comes to my attention while at [name of agency]. I will do this in accordance with the [name of agency]'s privacy policy and applicable laws, including those that require mandatory reporting.

I also agree to never remove any confidential material of any kind from the premises of [name of agency] unless authorized as part of my duties; with the express permission or direction to do so from [name of agency]; or as permitted or required by law.

_____
(Print Staff Name)

_____
(Signature of Staff)

_____
(Signature of witness)

Dated this _____ day of _____, 2_____

You can use the following text in a letter to a client. If it is appropriate in the circumstances (e.g., the breach is unlikely to result in someone else contacting your client before you do) an alternative is to use the text of this letter as the basis for a conversation with your client at his/her next scheduled appointment.

TEMPLATE: RESPONSE TO BREACH

Date

Name of Individual
Address
City, Province
Postal Code

Re:

Dear _____:

I am writing to tell you that we have reason to believe that your personal health information has been [choose one or more: lost/stolen/inappropriately accessed]. We have since investigated the situation, and have concluded that [provide small amount of detail about the circumstances, if appropriate].

We apologize for any concern this may cause you. [Name of custodian] takes issues related to individual privacy very seriously and we are committed to keeping our clients' personal health information safe and confidential. This incident has given us an opportunity to revisit our processes and to implement additional safeguards, so that this does not happen again.

If you have any questions or concerns, please do not hesitate to contact me. You may also make a complaint to the Information and Privacy Commissioner's Office at:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Tel: (416) 326-3333
Toll-free: 1-800-387-0073

Yours truly,

CHAPTER 3

This chapter provides an overview of hen you must get express (written or oral) consent, when you can rely on a client's implied consent, and when you are Allowed to collect, use or disclose PHI without consent. It also provides you with a checklist to follow when you need to make decisions about consent (including for capable or deceased persons), capacity and substitute decision-making.

Consent, capacity and substitute decision-making

KEY POINTS

A capable person of any age has the right to make his/her own decisions about the collection, use or disclosure of personal health information (PHI).

An individual who is capable and 16 years of age or older may designate someone else to make those decisions for him or her.

There are special rules about giving consent on behalf of a person who has died.

A capable person of any age is presumed to be capable of consenting to the collection, use or disclosure of their PHI. However, if a child is under the age of 16, a parent may also give consent on behalf of the child in certain circumstances. The rules in PHIPA are not the same as the rules in the *Health Care Consent Act*.

In some situations, it may not be reasonable to presume capacity. PHIPA creates a framework for substitute decision-making in cases where a person is found to be incapable of making these decisions.

Consent may be express (oral or written) or implied, unless the Act requires it to be express. In some cases, consent is not required at all for the collection, use or disclosure of PHI. Custodians and their agents need to pay special attention to these rules.

PHIPA REFERENCE

For more complete information, you should also look at the following sections of PHIPA: 18-28

Consent

In some cases, PHIPA requires that you have the consent of clients before collecting, using or disclosing their PHI. You can also refer to Chapters 4, 5 and 6 for more information on circumstances when you may proceed without consent.

Consent is valid under PHIPA if

- it is the consent of the individual (or of the appropriate substitute decision-maker, if there is one),
- it is knowledgeable (which can also be achieved by posting your notice of information practices, as discussed below),
- it relates to the information, and
- it is not obtained through deception or coercion.

When is consent knowledgeable?

PHIPA specifies that unless it is unreasonable in the circumstances, you may presume that your client knows why you are collecting, using or disclosing his/her PHI if you have posted or made readily available a notice describing those reasons. You must post it or make it available in such a way that your clients are likely to see and read it.

For example, you are required to prepare and make available a written public statement, such as a privacy notice, and that might be a good place to describe the purposes for which you collect, use or disclose PHI. As with other written materials prepared for the mental health and addictions communities, you may want to use a large, readable font in your notice and consider what may be the best timing and method of providing it to your clients. The Office of the Information and Privacy Commissioner has developed a series of “short notices” (posters and brochures) for the health care sector, which may help your clients to understand PHIPA. You can order free copies by sending an e-mail to info@ipc.on.ca or by telephone at 416-325-9172.

Where the *Act* does require consent, that consent can be express or implied, unless the Act requires express consent.

Express consent

Express consent is either written or oral. If the client gives you a written, signed consent, you should place it in the client's health record. If you get oral consent, you should also make a note of that in the health record.

You must get express consent if you are

- giving PHI to someone who is not a custodian (for example, a recipient under PHIPA, such as an employer, insurer or family member who is not the client's substitute decision-maker),
- giving PHI to someone who is a custodian, but for a purpose unrelated to health care (for example, to a nurse who reviews claims for an insurance company), or
- sharing PHI within your agency or giving it to a third party for marketing purposes (or for fundraising purposes, unless the conditions for relying on an implied consent are met).

Implied consent

You can rely on the client's implied consent for the collection, use and disclosure of

PHI in a number of situations under PHIPA, including any of the following:

- Any time PHIPA says consent of the client is required, unless it specifically says that the consent must be express (see "Express Consent" above). Once you have taken the steps to ensure that your client's consent is knowledgeable and the other criteria are met, as set out above, his/her consent may be implied.
- If you receive PHI from the client, his/her substitute decision-maker or another custodian for the purpose of providing health care or assisting in providing health care, unless you are aware that the client has specifically withdrawn or withheld the consent.
- For fundraising purposes, in very limited circumstances set out in the regulations to PHIPA.

You should never rely on implied consent if you have reason to believe that the client

- would not give consent, or
- gave consent previously but has since withdrawn it.

QUESTIONS AND ANSWERS

Q Does implied consent apply to interagency service agreements that are not mandated by law?

A Yes, if the service agreement is necessary to provide continuing care to the client and all of the participating agencies are health information custodians. If not, you will have to obtain the client's express consent before giving the PHI to that agency. You should also make sure that the client is aware that you are sharing his/her PHI with other agencies, through your written public statement; or if the client, his/her substitute decision-maker or another custodian gave you the PHI, you may give it to another custodian for health care purposes unless you are aware that the client has withheld or withdrawn the implied consent.

Any custodian that is part of an interagency agreement is required to comply with PHIPA, and the agreement could reflect that.

Clients can withhold or withdraw consent

Individuals have the right to withhold or withdraw their consent for the collection, use or disclosure of PHI in certain situations. This means that a client may tell you not to collect, use or disclose their PHI, and if PHIPA says that it is a situation that requires the client's consent, you must abide by that wish. For example, you must obtain express consent to give a client's PHI to an insurance company. The client is allowed to change his/her mind about having told you to disclose that information. In other situations, a client may decide not to consent in the first place. A withdrawal cannot be retroactive.

If the disclosure is for the purpose of providing health care, you have a responsibility to inform the other custodians to whom you are disclosing the PHI that you do not have the client's consent to give them information you think is relevant to the provision of health care. You are not allowed to provide any additional detail.

This type of withdrawal does not affect your right (and in some cases, responsibility) to use and disclose PHI without consent.

Your ability to use or disclose PHI without your client's consent (including mandatory reporting) will be discussed in Chapters 5 and 6. Any consent forms you use should state that consent may be withheld or withdrawn at any time. A sample consent form for disclosure of PHI is provided at the end of this chapter.

QUESTIONS AND ANSWERS

Q We have always obtained a client's express consent before sharing information with other health care providers. I am uncertain about the new rules about implied consent.

A There is nothing in PHIPA to prevent you from continuing to ask clients for their express consent to collect, use or disclose their PHI. However, PHIPA was intended to remove barriers to timely health care and duplication of services, by allowing custodians who are involved in the client's care to give each other PHI based on implied consent. You can do this unless you are aware that your client has specifically withheld or withdrawn his/her consent.

Clients have the right to withdraw implied consent, just as they would with express (oral or written) consent.

Consent and children

A young person has the right to make his/her own decisions about the collection, use or disclosure of PHI. If a child under the age of 16 has given his/her own consent under the Health Care Consent Act to treatment, or participated in counselling under the Child and Family Services Act, any information decisions relating to those two situations are the child's to make. Otherwise, the decision with respect to the collection, use or disclosure of the child's PHI may be made by either the capable child or, where the child is under 16, his/her parent.

If there is a conflict between the parent and the capable child who is under 16, the decision of the child overrides that of the parent.

If another person or a children's aid society has the legal right to make decisions in place of the parent, the parent has no right to make the decision. In the case of divorce or separation, a "parent" means the custodial parent, and not a parent who has only a right of access.

The following is a checklist of steps to consider when a situation involves consent, capacity and substitute decision-making under PHIPA:

CHECKLIST FOR CONSENT

1. Check to see that this is a decision about collection, use and disclosure of PHI

   PHIPA creates a framework for consent, capacity and substitute decision-making for the collection, use and disclosure of PHI.

   You may already be familiar with similar rules in the Health Care Consent Act that deal with consent to treatment, admission to a care facility (i.e., a long-term care home), and personal assistance services.

   The Health Care Consent Act is an Ontario law that many health care practitioners rely on often, because it tells them

   - when they must get consent for a proposed treatment,
   - when to assess whether a person is capable of deciding whether to accept or refuse a particular treatment, and
   - when to turn to a substitute decision-maker to make the decision.

   It is important to remember that the PHIPA rules are comparable to, but not the same as, the rules about treatment under the *Health Care Consent Act*.

2. Determine what type of consent you should get, if any.

   PHIPA tells you when you

   - need to get consent for collection, use or disclosure of PHI (implied or express),
   - need to get express consent for collection, use or disclosure of PHI (which can be written or oral),
   - are allowed to rely on the individual's implied consent, and
   - can collect, use or disclose PHI without consent.

3. Who will give the consent?

   A capable client, of any age, has the right to make his/her own decisions about the collection, use and disclosure of PHI.

   If there is a substitute decision-maker entitled to make decisions under the Health Care Consent Act for the client, that person automatically becomes the substitute decision-maker under PHIPA for information decisions that are necessary for, or ancillary to, the client's treatment.

There may be no substitute decision-maker for treatment under the Health Care Consent Act. In that case, if you determine that the client is incapable of making decisions about the collection, use or disclosure of his/her PHI, you must turn to the list of substitute decision-makers in PHIPA. (See below for further detail about capacity determinations.)

4. Consent of a capable person – the test

When you do obtain consent under PHIPA, the general rule is that it must be the consent of a capable person.

The test of whether or not a person is capable relates to

- his/her ability to understand the information that is relevant to making a decision about the collection, use or disclosure of PHI, and
- the ability to appreciate the reasonably foreseeable consequences of giving or not giving, withholding or withdrawing the consent.

A capable person may decide to make his/her own decisions, or ask that someone else make these decisions. In the latter case, the person must designate the other person in writing and both must be at least 16 years old. The person who is designated, however, can be either an individual, or an organization such as a trust company.

5. Assumptions you can make about consent and capacity

You can assume that a client is capable of giving consent under PHIPA. However, this should be a reasonable assumption, informed by the situation you are in.

You can assume that consent you receive (from the client or someone else) is valid consent, and the person giving it to you has the authority to act for the incapable client. Again, this has to be a reasonable assumption. It is always best to be alert to any indications of incapacity. When in doubt, you should also satisfy yourself that anyone who says he/she can provide consent for an incapable client has authority under PHIPA to do so.

6. Capacity determinations

If you have any doubts about the client's capacity, you should determine his/her capacity.
See below for helpful tips on determining capacity.

7. Rights advice

If you have found the client incapable under PHIPA, you must provide the client with information about the consequences of such a determination, if it is

reasonable under the circumstances to do so. The client may challenge the finding of incapacity to the Consent and Capacity Board.

While there is no official standard, it is likely that many custodians in addictions and mental health settings will provide this type of information to their clients.

8. Consent on behalf of an incapable person

PHIPA provides a ranking of substitute decision-makers who have the right to give, withhold or withdraw consent on behalf of an incapable person:

1. The individual's guardian of the person or guardian of property, if the consent relates to the guardian's authority to make a decision on behalf of the individual.
2. The individual's attorney for personal care or attorney for property, if the consent relates to the attorney's authority to make a decision on behalf of the individual.
3. The individual's representative appointed by the Consent and Capacity Board, if the representative has authority to give the consent.
4. The individual's spouse or partner.
5. A child or parent of the individual, or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent. This paragraph does not include a parent who has only a right of access to the individual. If a children's aid society or other person is lawfully entitled to consent in the place of the parent, this paragraph does not include the parent.
6. A parent of the individual with only a right of access to the individual.
7. A brother or sister of the individual.
8. Any other relative of the individual.

The Public Guardian and Trustee has discretion to act as the substitute decision-maker only if no one in the list above can fulfill that role.

9. Express versus implied consent

In most cases, where PHIPA requires you to get your client's consent, the consent may either be express (written or oral) or implied. However, as discussed above, there are a few circumstances where the consent cannot be implied, and you must get express consent.

Clients should understand that consent may be withdrawn, or that they may choose not to give it in the first place.

10. Documentation of consent

When you do get a client's consent, it is important that it be documented. This could be a written consent signed by the client, or a documentation of the fact that the client gave you oral consent. You must also follow any standards for documentation of your professional college or other body that has provided you with a licence.

Consent in other situations

If a person is capable

Anyone who is mentally capable of making a decision about the collection, use or disclosure of his/her PHI may do so. Otherwise, if he/she is at least 16 years old, he/she may ask someone else to make those decisions by putting that request in writing.

The rules for decisions on behalf of children have already been explained above. Another law may also give the authority for someone to act on behalf of the client.

If a person has died

An estate trustee (someone who is named in a legal will or who has applied to a court for this formal designation) may make these decisions on behalf of a person who has died. If there is no estate trustee, that authority goes to the person who has assumed responsibility for the deceased person's estate. (This may be either a formal appointment; but often, it is a family member of the deceased person who has taken on key responsibilities.)

SHARING PHI WITH A CLIENT'S HEALTH CARE PROVIDERS[1]

PHIPA allows custodians who are providing health care, or assisting in providing health care to a particular client, to share or disclose the information they need in order to provide that care. You can do this based on the client's implied consent.

The client has the right to tell you not to share or disclose this information, and under the "lockbox" provisions (discussed in Chapter 6), you will have to honour that request unless you are permitted or required under PHIPA or another law to continue to share it or disclose it.

If the client asks you not to disclose specific PHI to another custodian and you think what is missing is relevant to the other custodian's ability to provide health care to the client, you must advise the custodian that they are not receiving all PHI that, in your opinion, is relevant to care. You may also wish to discuss with the client the implications of shielding this PHI, and try to find out what he/she is concerned about.

If you feel that another custodian is not sharing PHI that can and should be shared between custodians to assist a client's health care, there are at least two possible reasons:

- Prior to PHIPA, sharing certain client information required express consent; the other custodian's staff members do not want to disclose PHI to you because they are unsure who is covered under the new rules.
- The other custodian has made a decision that in spite of what PHIPA allows, clients' express consent will still be required before staff members will release the PHI.

Try to find out which situation applies and what the other custodian's concerns are. Ideally, you will be able to work together to arrive at a solution that suits everyone, keeping in mind that one of PHIPA's goals is to reduce barriers to care, including information barriers.

[1] This is sometimes referred to as the client's "circle of care." This term is not used in PHIPA, but has been widely adopted in the health care community. Unfortunately, it sometimes leads to confusion about who falls under PHIPA. PHIPA is very specific in its definitions of "health information custodians," "health care," "personal health information," "use" within a custodian, and "disclosure" to those outside the custodian. These definitions, with reference to people's primary functions, should guide you in determining how widely a client's PHI should be shared. See the Information and Privacy Commissioner's guidance on the subject here: https://www.ipc.on.ca/wp-content/uploads/Resources/circle-of-care.pdf (August 2015).

QUESTIONS AND ANSWERS

Q We know that the real focus these days is on system coordination, and making appropriate referrals for high needs clients. At the same time, lots of personal health information is being shared more freely than we expected, to facilitate these referrals. Sometimes this includes sharing of information about individuals with another agency, about individuals who are not their clients. How does PHIPA affect this practice?

A In the past, this was sometimes referred to as granting "privileges" to certain community partners, in part to remove barriers to health care and promote the appropriate sharing of information among a client's health care providers. The language of "privileges" is no longer terribly current. And it is potentially problematic under PHIPA.

Under PHIPA, most health care organizations have adopted a "need to know" policy: information is shared with those actively involved in a client's care. As a reminder, you should anonymize information (or minimize the amount of PHI you use) where possible. You should take care not to disclose PHI if it is not necessary for someone to carry out their functions.

It is important that in any situation (such as rounds) where a number of clients are being discussed, you consider who is involved in each client's care. If a social worker is not involved (and is unlikely to be involved because of staff coverage/vacation issues), you may want to change your way of doing things to limit who attends.

The Act does permit a health information custodian to share PHI with its agents for the purposes of educating them to provide health care. Sharing case findings for the purposes of education is fine, as long as the person receiving the information is an agent of the health information custodian. (And to be an agent, you must be collecting, using or disclosing PHI on behalf of that custodian, not for your own purposes.)

TEMPLATES

TEMPLATE: RELEASE OF INFORMATION

Pursuant to the *Personal Health Information Protection Act, 2004* (PHIPA)

I, _____,
(Print your name)

authorize _____
(Print name of health information custodian)

to disclose
□ **my personal health information consisting of:**
_____

_____

(Describe the personal health information to be disclosed)

or

□ **the personal health information of**

_____

(Name of person for whom you are the substitute decision-maker*)

consisting of:_____

_____

(Describe the personal health information to be disclosed)

to _____

(Print name and address of person requiring the information)

I understand the purpose for disclosing this personal health information to the person or organization noted above. I understand that I can refuse to sign this consent form or later withdraw my consent.

My Name: **_____**

Address: _____

Home Tel.: _____ Work Tel.: _____

Signature: **_____** Date: **_____**

***Please note:** A substitute decision-maker is a person authorized under PHIPA to consent, on behalf of an individual, to disclose personal health information about the individual.

TEMPLATE: CAPACITY DETERMINATION FORM

An individual's consent is required for the collection, use or disclosure of personal health information and must

- be from the individual or someone authorized under PHIPA to make decisions on his/her behalf,
- be knowledgeable,
- relate to the information, and
- not be obtained through deception or coercion.

An individual is capable of giving this consent if he/she is able

- to understand the information that is relevant to deciding whether to consent to the collection, use or disclosure, as the case may be, and
- to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing the consent.

If a client's capacity is in question, the client's capacity should be reviewed by a health professional or social worker on the staff of [insert name of agency] who is most closely associated with the client's care. The determination is to be conducted in a professional and objective manner. The methodology used and the information relied on must be documented in the client's file. Once the determination has been conducted, the [insert name of agency] staff person is to complete this form and submit a copy to [appropriate person within your agency, if any].

COMPLETED BY: _____
Staff name

_____
Staff title

CLIENT'S FULL NAME: _____

DATE OF MEETING WITH CLIENT: _____

Assessment:

CHAPTER 4

This chapter tells you about collection of PHI, and when you are allowed to collect it from someone other than the client.

Collecting personal health information

KEY POINTS

The general rule is that the individual must consent to the collection of his/her personal health information (either express or implied).

Custodians and their agents may only collect information indirectly (from a person other than a client or his/her substitute decision-maker) with the consent of the individual (or his/her substitute decision-maker, where relevant), or in other limited and specific situations.

PHIPA REFERENCE

For more complete information, you should also look at the following section of PHIPA: 36

Definitions and rules

What is collection?

You “collect” PHI when you gather, acquire, receive or obtain it, regardless of how, or from whom, you get it.

Collecting with Authority

You must take reasonable steps to ensure that PHI is not collected without authority.

Collecting PHI from someone other than your client

You are allowed to collect PHI indirectly (from someone other than your client) if,

- you have the consent of the client, or the client’s substitute decision-maker,
- you have the authority under PHIPA or another law to do so,
- a law permits or requires another person to disclose the PHI to you,
- the Information and Privacy Commissioner has said that you can (but so far, there have not been any Commissioner’s rulings that would allow this),
- you need the PHI in order to provide care to the client, but cannot get the information from the client either in a timely way or accurately or completely, or
- you have the approval of a Research Ethics Board in limited situations related to research (this is usually done by teaching and other hospitals).

When can you not use PHI collected indirectly?

Even if you have collected PHI from a third party as allowed under PHIPA, there may still be limits on what you can do with that information once you have it. For example, a client has the right to instruct you not to use PHI if you collected it from someone else because you could not get timely or accurate information directly from the client in order to provide appropriate health care to the client. A second exception is where you collected the PHI with the client’s consent, and he/she is now withdrawing that consent. The client’s ability to shield this information is commonly referred to as the “lockbox,” although that word does not appear in PHIPA. [There will be more discussion of this in Chapter 6.]

What this means is that if the client tells you not to use PHI you collected from a third party (such as the client’s neighbour or friend) in order to provide health care to the client, you will have to accommodate that request. This could also mean having to shield the information from others at your agency, including members of the client’s health care team.

QUESTIONS AND ANSWERS

Q A client's family member often volunteers information about the client that his clinical team thinks is important. I know that in most cases, we have to keep the client's information confidential, but is it okay to listen to what his family has to say?

A You can collect PHI from anyone, if you have the client's consent.

Otherwise, you need to consider whether one of the other exceptions applies. Do you have any legal authority to collect the PHI from someone else, for example, on a Form 1 under the Mental Health Act? Or, do you need the information in order to be able to care for this client? (AND you can't get it directly from the client OR you have concerns about the client being willing or able to give you reasonably accurate and timely information?)

If either of those scenarios applies to your situation, you can collect PHI from the family member, or anyone else, without the client's consent. But there is a catch.

Given the amount of intake and referral that goes on in the community mental health and addictions fields, staff must be able to collect information that is clinically relevant. You should always remember that if you collected PHI on the basis that the client cannot or will not give you timely or accurate information, he/she is free to later instruct you not to use the information for the purpose for which you collected the PHI in this way. Further discussion of what is sometimes informally referred to as the "lockbox" in PHIPA is found in Chapter 6 of this Toolkit.

Q A client's neighbour called and told one of our therapists that the client has spent the last two weeks in jail but is now out. At the next therapy session, the client says he was away because of a family emergency.

Should the neighbour's information be put in the notes?

Could this have an impact on the neighbour's safety?

How should the therapist handle treating the client with confidential knowledge that is not "on the table" in therapy?

A Although the staff member did not ask for this information, it is still a collection of PHI under the Act.

In this case, the staff member did not have the client's consent to collect the information, nor did it fall under most of the exceptions. For example, no other law allowed it, nor did the Information and Privacy Commissioner create a new rule to permit its collection.

The only exception that might apply is if the staff member believes that the fact that the client was in jail is relevant clinical information that could not be obtained accurately from the client, nor be obtained in a timely way.

Part of the philosophy behind PHIPA is that individuals have a right to control their PHI. However, staff cannot always anticipate what a family member or other third party may tell them about a client. The best approach may be to make every effort not to collect PHI indirectly from third parties. If and when it happens, document it, and be aware that the client could later instruct you not to use the information you collected from the neighbour (by invoking what is sometimes informally referred to as the "lockbox," which will be discussed further in Chapter 6).

Once you have the information, it should be documented, particularly where the information is related to potential risk. The rules in PHIPA about a client's right of access to his/her record of PHI also contain a number of exceptions, including where letting the client see the record could be harmful to the client's treatment or recovery or would create a risk of harm to a third party; or the person who provided the information expected it to be kept confidential.

CHAPTER 5

This chapter explains what it means for you to “use” PHI, when you are allowed to use it without consent, and when you cannot use it.

Sharing PHI within your agency

KEY POINTS

Custodians and their agents should be familiar with the difference between “using” and “disclosing” personal health information (PHI).

PHI can be used without client consent in specific circumstances that are set out in PHIPA.

If you have collected PHI about a client because you reasonably needed the information to provide health care and you could not get the information you needed from the client accurately or in a timely fashion, the client can instruct you not to use that information (sometimes referred to informally as a “lockbox” for use).

Also, if you collected the PHI about a client without consent, the capable client (or where applicable, his/her substitute decision-maker) may instruct you not to use it for the purpose for which you collected it.

PHIPA REFERENCE

For more complete information, you should also look at the following

section of PHIPA: 37

What is the difference between a “use” and a “disclosure” of PHI?

PHI is “used” when it is shared between a custodian and agent, or among the agents of a custodian. For example, if a staff member of an agency shares a client’s PHI with one of the social workers who works with the agency, the information is being used. This is different than a “disclosure,” which happens when you give the PHI to someone who is not collecting, using or disclosing PHI on behalf of the agency.

The definition of “use” has been revised by Bill 119, and viewing PHI is now also considered a “use”.

As mentioned in the first part of the Toolkit, the agents of a custodian include staff, health care practitioners, volunteers, students, researchers and independent contractors.

Uses of PHI

As a custodian of PHI (or an agent of a custodian), you are allowed to use PHI for a number of purposes without having to get your client’s consent. Most of these uses relate to supporting and improving the programs and services you offer. One of the main purposes of PHIPA is to allow PHI to flow appropriately within the health system to enhance the care and services given to clients.

You can use PHI without client consent in the following situations:

- For the purpose for which the information was created and all functions related to the purpose (but you cannot use it if the client previously consented to a collection and now withdraws the consent; or if you collected it indirectly for health care purposes, from someone other than the client, and the client tells you not to use it)
- For risk management
- For other activities to improve the quality of your programs or services (an example might be chart audits to ensure that staff are documenting properly)
- In order to get consent from a client
- For purposes of disposing of the information (such as hiring a shredding company) or in order to de-identify the information
- To share information with staff to provide better care to clients
- To plan or deliver programs or services that you provide to clients, or if you are funding other programs or services and need to allocate resources or monitor for fraud
- In order to obtain payment for health care services
- For research conducted by the custodian without consent, as long as you have followed the research rules in PHIPA (section 44, which includes getting Research Ethics Board approval)
- If you or your agent are a party or witness in a proceeding (or anticipated proceeding) before a court or tribunal, such as a Consent and Capacity Board or the Ontario Review Board; at an inquest; or as part of a regulated college’s review of a member’s conduct, such as a physician, psychologist, nurse or social worker

- In order to educate your agents to provide health care (for example, if you are training a new drug counsellor)
- For any other purpose allowed under PHIPA or another law (or by a treaty, agreement or arrangement made under a law of Ontario or Canada)

In spite of all of the uses of PHI that are allowed under PHIPA without the client's consent, you are still free to ask for consent. It is important for custodians to think about whether they will rely on all of the uses that PHIPA authorizes without having to get consent. What should be clear, though, is that if you do ask for a client's consent, he/she may give it; not give it (which means you will not be able to use the PHI); or give it and then change his/her mind. Through your written public statement (discussed in Chapter 2) you will need to be clear about why you collect, use and disclose PHI, and when you will ask for consent.

If you use (or disclose) a client's PHI in a way that is outside the scope of your information practices that you have already made available through your written public statement, you must

- tell your client about the uses and disclosures (unless they relate to a record of PHI the client would not have a right to access), and
- make a note of the uses and disclosures in the client's record of PHI (or in a way that can be linked to the record).

If you are an agent of a custodian, you should familiarize yourself with your agency's privacy policies and other expectations about privacy and PHIPA.

QUESTIONS AND ANSWERS

Q Six months ago, we provided training to staff on how and what to document in the client's health record. I want to do a random audit of client records to assess whether the training was successful and appropriate data is being captured.

Is this a use of PHI? Do I have to get the consent of clients whose charts will be reviewed?

Is this type of review "research" under PHIPA, and if so, do I have to take any special steps such as getting approval from a research ethics board?

A This is, in fact, a use of PHI.

PHIPA allows you to use PHI without consent for the purpose of improving or maintaining the quality of care you provide, and of your programs and services. You should find out whether this is what your agency's, i.e., does the agency have an internal process for authorizing this use, or are its agents free to do so without any vetting of the quality improvement exercise?

This is different than using PHI for "research" without consent, which requires you to comply with the detailed research rules set out in PHIPA. This would include getting approval of a research ethics board. (Most of the time, this type of research is done through teaching hospitals or other health facilities.)

CHAPTER 6

This chapter tells you when you can or must give ("disclose") a client's PHI to someone who is not your agent. It describes when you must get a client's express consent, when you can rely on his/her implied consent, and when you can disclose the PHI without consent.

Disclosure: Giving personal health information to someone outside your agency

KEY POINTS

You have the right under PHIPA to disclose personal health information (PHI) about a client based on express (oral or written) consent, implied consent, or in some cases, without consent.

In a few cases, the consent must be express.

You should be familiar with the circumstances where you have the discretion to disclose PHI without consent, for example, when PHIPA or another law permits or requires you to do so; when you participate in a proceeding such as a court or tribunal hearing; and for the purposes of eliminating or reducing a significant risk of serious bodily harm to your client or another person.

If a client, his/her substitute decision-maker or another health information custodian gives you PHI about the client, you can rely on implied consent to disclose it for the purposes of health care or assisting in health care of the individual, unless you are aware that the client has withdrawn or withheld consent. However, clients do have the right to tell you not to disclose their PHI to other health information custodians in limited circumstances related to providing them with health care (sometimes referred to informally as a "lockbox," a term that is not actually in PHIPA).

You may charge a fee for disclosure of a client's PHI to someone who is not your agent, but unless and until regulations are made under PHIPA to specify the amount of that fee, you must limit it to reasonable cost recovery. Regarding its Order HO-009, which speaks to reasonable cost recovery, the Information and Privacy Commissioner noted:

> There is currently no regulation that sets the fee amount for providing access to an individual's records of personal health information. However, our Health Order HO-009 interpreted reasonable cost recovery and found that a custodian may charge a fee of $30 for photocopying or printing the first 20 pages of a record and 25 cents per page for every additional page. This $30 fee 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. (https://www.ipc.on.ca/health/access-and-correction/)

A parallel decision on fees for release of records of PHI to a third party such as a lawyer was later issued (Decision 14). In this case, the Information and Privacy Commissioner held that higher fees were not justified for disclosure to a third party, but that the reasoning in Order HO-009 should be followed. In other words, a client should not pay more to access his/her records than would be paid for releasing those same records to his/her lawyer.

PHIPA REFERENCE

For more complete information, you should also look at the following sections of PHIPA: 38-50

Background

By now, you should be familiar with a number of concepts that are important to the “disclosure” of PHI:

- When is someone an “agent” of a custodian (Chapter 1)
- The difference between “use” and “disclosure” of PHI (Chapters 5 and 6)
- Consent for collection, use and disclosure of PHI (Chapter 3; also see Chapters 4, 5 and 6)

From time to time, your clients may ask you to release their PHI to third parties (that is, another health information custodian or a non-health information custodian). You may also receive requests directly from third parties asking that you give them your client's PHI. The general rule is that you can only disclose your clients' PHI to someone who is not an agent of your organization if the law either allows or requires you to do so

- with your client's consent (in some cases, it must be express; in others, the law permits you to rely on implied consent), or
- without consent.

Disclosure by your agents

The general rule is that your agents may disclose PHI where you would have the authority to do so under PHIPA, as long as you have specified this as part of their duties. However, there is an exception. An agent may disclose PHI without your permission if permitted or required by law to do so, including under the regulations to PHIPA.

When do I need to get my client’s express consent?

You must get a client’s express (written or oral) consent if you are giving the PHI to someone

- who is not a custodian (for example, an employer) and the law does not allow a disclosure without consent,
- who is a custodian but who is not going to use the PHI for a health care purpose and the law does not allow a disclosure without consent, or
- for marketing purposes (or if, for fundraising purposes, you plan to give more than the name and address of your client and his/her substitute decision-maker).

A written consent is always best. If the client gives you an oral consent, make sure to document it (including when and how it was given).

When can I rely on my client's implied consent for disclosure?

Please refer to Chapter 3 of the Toolkit for the circumstances in which you can rely on an implied consent for disclosure.

Disclosing PHI without consent

There are a number of circumstances where you do not have to get consent in order to give PHI to someone outside your agency:

- PHIPA or another law gives you the right or requires you to disclose PHI. There are a number of laws that give you the authority or require you to give PHI to someone else. (Examples include mandatory reporting of specific communicable diseases to public health authorities under the Health Protection and Promotion Act and the duty of physicians and optometrists to report their opinion that a client is suffering from a condition that makes it dangerous to drive, to the Registrar of *Motor Vehicles under the Highway Traffic Act.)*
- For health or other programs (including to determine or verify eligibility for health care and other services that are funded by the government; audits and accreditations of the custodian's services; prescribed persons who maintain a registry of PHI for facilitating or improving health care; another custodian who provides or assists in the health care and for the purpose of improving the quality of care provided)
- In proceedings including those of a court or tribunal
- For planning and management of the health system, to designated organizations whose information practices have been approved by the Information and Privacy Commissioner (prescribed entities)
- For research, under specific conditions: if you are considering giving PHI to an outside researcher, you will need to make sure that you have taken a close look at the rules under section 44 of PHIPA
- In circumstances related to risk (where it is necessary to eliminate or reduce a significant risk of serious bodily harm to your client or to another person, discussed further below)
- To assist in a client's placement in a facility for health care purposes
- To assist in placing an individual into a custodial setting, such as under the Criminal Code mental disorder provisions

As mentioned above, a custodian may disclose PHI about a client to another custodian, without consent, if both custodians are currently providing health care to that client (or if both custodians did so in the past) and the custodian that receives the PHI will use it to conduct activities that improve or maintain the quality of care it provides, either to that same client or to another client in a similar situation. This allows you to share PHI about a client with another custodian, who might then use that PHI to provide health care to a client unrelated or unknown to the client whose PHI was disclosed. When doing this, it is important to consider how and what information will assist you in providing health care to another client in a similar situation. It is recommended that you take

precautions to disclose only the PHI that would be necessary to provide quality care and not to disclose PHI that would not be helpful to improving care provided to that or another client.

Mandatory disclosure

The following chart was originally developed by the hospital sector and its partners in order to give an overview of when PHI may be disclosed without consent under PHIPA.[1] It has been adapted for the mental health and addictions communities, with new additions in the 2017 version of the Toolkit. This is a starting point for understanding the many disclosures without consent that PHIPA allows; however, the list is not exhaustive and you should consult the Act for further detail.

The Act specifically permits the disclosure of PHI for a number of purposes as required by other statutes. Consent is not required for these specific purposes. For example, you are required to provide the following information:

To Whom Disclosure Must Be Made	What Information Must Be Disclosed	Authority
Aviation Medical Advisor (Note that this is a mandatory disclosure for physicians and optometrists)	Information about flight crew members, air traffic controllers or other aviation licence holders who have a condition that may impact their ability to perform their job in a safe manner	*Aeronautics Act*
Chief Medical Officer of Health or Medical Officer of Health	Information to diagnose, investigate, prevent, treat or contain communicable diseases	*Health Protection and Promotion Act* *Personal Health Information Protection Act*
Children's Aid Society	Information about a child in need of protection (e.g., abuse or neglect)	*Child and Family Services Act*
Registrar of College of a regulated health care profession	1. Where there are reasonable grounds to believe a health care professional has sexually abused a patient, details of the	*Regulated Health Professions Act*

[1] Ontario Hospital Association (OHA), Publication # 314, September 2004. Reproduced with the permission of OHA and its partners, the Ontario Ministry of Health and Long-Term Care; the Ontario Hospital Health Council; the Ontario Medical Association; and the Office of the Information and Privacy Commissioner.

To Whom Disclosure Must Be Made	What Information Must Be Disclosed	Authority
(Note that this is a mandatory disclosure for health care professionals regulated under the RHPA and for facilities that employ regulated health care professionals.)	allegation, name of the health care professional and name of the allegedly abused patient • The patient's name can only be provided with consent • You must also include your name as the individual filing the report. 2. Where there are reasonable grounds to believe that a health care professional who practices at that facility is incompetent or incapacitated. Report only required if professional's name is known 3. Termination or suspension of employment of a health care professional for reason of the practitioner's professional misconduct, incompetence or incapacity or where termination was imminent and professional resigned	
Coroner or designated Police Officer	Facts surrounding the death of an individual in prescribed circumstances (e.g., violence, negligence or malpractice) Information requested for the purpose of an investigation	*Coroners Act*
Police (Physician's duty to report)	Where physician issues order for examination in the context of a community treatment	*Mental Health Act*

To Whom Disclosure Must Be Made	What Information Must Be Disclosed	Authority
	order: name, address and telephone number of physician who is to perform the examination, if the client attends, and if the order is revoked prior to its expiry	
Officer in Charge of a Psychiatric Facility, if applicable Any person named in the community treatment plan (Physician's duty)	To give copy of Community Treatment Order (Form 45)	*Mental Health Act*
Medical Officer of Health of Public Health Unit in area where services were provided (duty to report for physicians, chiropractors, nurses, dentists, pharmacists, optometrists and naturopaths)	Where patient has or may have a communicable diseases that is reportable under the Act Patient's full name and address, full date of birth, sex, and date of onset of symptoms and any additional information required under the Act or requested by the Medical Officer of Health	*Health Protection and Promotion Act*
Minister of Transport (Federal)[2] (Duty of physician and optometrist)	Reasonable grounds to believe that the holder of a certificate issued under the Act has a medical or optometric condition that is likely to constitute a hazard to maritime safety. Must include	*Canada Shipping Act*

[2] Mandatory and Permissive Reporting, College of Physicians and Surgeons of Ontario Policy #6-12, updated December 2012.

To Whom Disclosure Must Be Made	What Information Must Be Disclosed	Authority
	opinion and information on which it is based	
Order, warrant, writ, summons, subpoena or other process issued by an Ontario court	Information outlined on the warrant, summons, etc.	*Personal Health Information Protection Act*
Registrar General	Births and deaths	*Vital Statistics Act*
Registrar of Motor Vehicles (Note that this is a mandatory disclosure for physicians and optometrists only)	Name, address and clinical condition of a person who has a condition that may make it unsafe for them to drive (Note that this duty will be amended when section 55 of the *Transportation Statute Law Amendment Act, 2015* c.14 is proclaimed in force)	*Highway Traffic Act*
Workplace Safety and Insurance Board	Information the Board requires about a patient receiving benefits under the *Workplace Safety and Insurance Act*	*Workplace Safety and Insurance Act*

Disclosure for health-related programs and legislation

The following tables outline examples of where PHI may be disclosed. See also the “Consent” section for additional information on permitted disclosures.

Person Requesting Health Record or Patient Information	Purpose	Consent Needed	Authority to Release Information
Ambulance services operator or Delivery agent or the Minister	Administration/enforcement of the *Ambulance Act*	No	*Ambulance Act*

Person Requesting Health Record or Patient Information	Purpose	Consent Needed	Authority to Release Information
Cancer Care Ontario, Canadian Institute for Health Information, Institute for Clinical Evaluative Sciences or Paediatric Oncology Group of Ontario	To analyze or compile statistical information	No	*Personal Health Information Protection Act* regulations
Chief Medical Officer of Health, Medical Officer of Health or a physician designated by the Chief Medical Officer of Health	To report communicable diseases	No	*Health Protection and Promotion Act*
College of Pharmacists Investigator	Administration/enforcement of the *Drug Interchangeability and Dispensing Fee Act*	No	*Drug Interchangeability and Dispensing Fee Act*
College under the *Regulated Health Professions Act*, or *Social Work and Social Service Work Act*	Administration/enforcement of the relevant statutes	No	*Personal Health Information Protection Act*
Individual assessing patient capacity, who is not providing care to the patient	To assess capacity under the *Substitute Decisions Act*, *Health Care Consent Act*, or *Personal Health Information Protection Act*	No	*Substitute Decisions Act; Health Care Consent Act; Personal Health Information Protection Act*
Inspector	Enforcement of the *Drug and Pharmacies Regulation Act*	No	*Drug and Pharmacies Regulation Act*
Public Guardian and Trustee	To investigate an allegation that a patient is unable to manage their property	No	*Personal Health Information Protection Act*

Person Requesting Health Record or Patient Information	Purpose	Consent Needed	Authority to Release Information
Public Guardian and Trustee (PGT), Children's Lawyer, Residential Placement Advisory Committee, Designated Custodian, Children's Aid Societies	To carry out their duties and, for the PGT, to investigate serious adverse harm resulting from alleged incapacity	No	*Personal Health Information Protection Act*

Disclosure to lawyers, insurance companies, adjusters and investigators

Person Requesting Health Record or Patient Information	Purpose	Consent Needed	Authority to Release Information
Lawyers, Insurance Companies, Adjusters on behalf of a patient	To assist a patient with a claim or proceeding	Yes	Express Consent
Lawyers, Insurance Companies, Adjusters, Investigators, where agent or former agent of custodian is, or is expected to be, a witness or party to the proceeding and the requested PHI relates to or is a matter in issue in the proceeding or contemplated proceeding	To assist the agent or former agent of the custodian	No	*Personal Health Information Protection Act*

Disclosure to legal authorities and law enforcement

Person Requesting Health Record or Patient Information	Purpose	Consent Needed	Authority to Release Information
Head of penal or custodial institution or an officer in charge of a psychiatric facility where the patient is being lawfully detained	To assist with health care or placement decisions	No	*Personal Health Information Protection Act*
Investigator or Inspector (including police)	To conduct an investigation or inspection authorized by a warrant or law	No[3]	*Personal Health Information Protection Act*
Police without a warrant	Legal authorities and law enforcement	Yes[4]	Express consent
Police without a warrant	Where there are reasonable grounds to believe that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm	No	*Personal Health Information Protection Act*
Probation and Parole Services	Legal authorities and law enforcement	Yes	Express consent

WHAT IS A "LOCKBOX"?

Background and timing

[3] There has been considerable debate about the ability of health information custodians to disclose PHI to police. The Information and Privacy Commissioner has noted that a warrant is not necessary if the information is being given in the course of a police investigation. However, some custodians are taking the position that express consent or a warrant is the best approach, with very limited exceptions (for example, where there would be true obstruction of police, such as when they are about to make an arrest). If you remain uncertain about your ability to provide client information to police, you should seek legal advice.

[4] See footnote 3.

The term “lockbox” does not appear in PHIPA, but is widely used to refer to the ability of clients to control their PHI. The lockbox is now available to clients of community mental health and addictions programs and services. The lockbox did not apply to public hospitals until November 1, 2005, but does apply to mental health and addictions centres, programs or services.

Clients in all health settings (including hospitals, although there is an exception set out in s. 35(2) for patients in mental health facilities detained under the Mental Health Act or Part XX.1 Criminal Code forensic provisions) have the right to “lock” their PHI by expressly withdrawing their implied consent for its collection, use and disclosure. They may only do this where they are entitled to give consent under PHIPA.

When does it apply?

The lockbox only applies in limited circumstances under PHIPA, and does not affect the numerous circumstances in which a custodian has the right to use or disclose a client’s PHI without consent. The default is that you have the right to give a client’s PHI to another custodian for the purpose of providing health care. You cannot do so, however,

- unless it is reasonably necessary to do so, and
- it is not reasonably possible to get your client’s consent in a timely way, or
- if a client instructs you not to.

For example, a client may tell you not to disclose specific PHI to anyone who is providing him/her with health care, or more likely, that it not be given to a particular health care practitioner, such as a therapist or counsellor.

When does it not apply?

In spite of the lockbox, if another part of PHIPA allows or requires you to share or give this information, the client cannot use the lockbox. A few examples are where another law requires you to disclose specific information, such as to public health authorities under the Health Protection and Promotion Act, to consider whether your agency may be part of a community treatment plan under the community treatment order provisions of the Mental Health Act, or to comply with a duty to report suspected child abuse under the *Child and Family Services Act.* You also have the right (but are not required under PHIPA) to disclose PHI where the disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm. (See below for more on this issue.) A third example is the disclosure of PHI where you or your agent will be a party or a witness in some type of proceeding, such as a court or tribunal hearing, or a coroner’s inquest. The definition of “proceeding” in the Glossary provides further detail on this issue.

The lockbox has no impact on these and other permitted or required disclosures under PHIPA.

Do I need to inform clients of the ability to “lock” their PHI?

PHIPA does not require that you provide this information to your client, but does require you to respond to his/her request if the Act permits your client to ask that you “lock” specific information. Again, this can only happen in the context of health care, and does not affect the many other uses and disclosures that PHIPA permits without consent. And keep in mind, a client may not use the word “lock” or “lockbox” so it is important that your staff understand the nuance of what a client is asking.

Duty to inform another custodian

If you are giving PHI to another custodian and believe that the PHI that the client has “locked” is reasonably necessary for the client’s health care, you must notify the other custodian of the fact that some of the information has been locked by the patient and is not being provided. You must do so without telling the other custodian what information is missing.

Keeping the lines of communication open

It is always wise to talk to your clients about why they are reluctant to share potentially important information with others in your agency for health care purposes, or with their health care providers outside the agency. Of course, this should be done in a way that does not coerce the client into withdrawing the request for the lockbox.

You should explain to the client the potential impact of not allowing those who provide him/her with health care to have the information that allows them to provide better care. This could include: limits on the type of services the client will be able to receive, duplication of services, and a greater number of health care providers collecting the same information from the client. It is important, however, that these discussions not be, or be seen as, an attempt to coerce clients into accepting health care or services that they do not wish to have.

How specific can my clients’ requests be to “lock” their PHI?

The IPC suggests that to ensure that no PHI is mistakenly shared, it is important that custodians record any express instructions or limitations on consent to the collection, use or disclosure of PHI. Please visit the Commissioner’s website at www.ipc.on.ca for any updates (Fact Sheet #8 on Lock-box is here: https://www.ipc.on.ca/wp-content/uploads/Resources/fact-08-e.pdf.)

You should be proactive and consider how you would handle a very detailed request from a client to shield some but not all of his/her PHI; shield certain encounters and not others; or shield from some health care providers and not others. While there is no legal requirement to make known the right to lock one’s

PHI, you should certainly be ready to explain to the patient the limitations on requesting a lock-box, as well as its implications:

- Locking one's PHI may mean that in future, it cannot be accessed by another health care practitioner who needs to provide optimal care
- Requesting a lock-box does not prevent any other uses or disclosures of PHI that are permitted or required by law, whether PHIPA or another statute

QUESTIONS AND ANSWERS

Q Does PHIPA create a duty to warn?

A No. PHIPA gives custodians the right to disclose PHI if the disclosure is necessary to reduce or eliminate a significant risk of serious bodily harm to the individual or to another person. is a discretion, not a duty.

Disclosure is not mandatory. However, health care practitioners should also be familiar with the requirements of the health regulatory bodies that govern their practice, some of which have adopted a duty to warn in specific circumstances as a standard of practice.

Custodians should consider in advance when they might anticipate having to rely on their discretion to warn under PHIPA, and who will exercise the discretion. Any reliance on this section of PHIPA should be carefully documented in the health record, citing s. 40(1) of PHIPA. These are decisions that you should make in consultation with a clinician, if time permits; but privacy should never cost lives and this provision is meant to address that fact.

Q What steps should I take when I get a request from a third party to disclose my client's PHI?

A You should satisfy yourself that the person who is asking for the information has the legal authority to obtain it.

PHIPA does give you the right to assume that consent given to you is valid. For example, if the person says he/she is the client's highest- ranking substitute decision-maker under the Health Care Consent Act, you have the right to rely on the consent.

Nonetheless, many custodians take further steps, such as asking for written documentation such as a power of attorney for personal care if one has been given by your client. In all cases, documenting from whom you obtained consent, and what authority that person provided, is important.

If this is a situation that requires the express consent of your client, you should confirm that the client or his/her substitute decision-maker has consented to release the information.

If the third party provides you with the client's signed consent, you may rely on it. Again, many custodians do take the extra steps to ensure that it is in fact the client's consent by checking the signature against one on file and/or by contacting the client or substitute decision-maker if appropriate.

In cases where PHIPA gives you the right to rely on implied consent, some custodians use a callback system to test whether callers requesting information are who they say they are. While this is not a foolproof system, it is one step of several to gather the information you need before you can release information.

Even if you are required to produce a record of your client's PHI for a proceeding (such as a court or tribunal hearing), you should never send it by mail. Instead, you should take it to the proceeding and wait for direction from the court or tribunal.

Other important things to know

Fees

You can only charge a fee for disclosing PHI to third parties that amounts to cost recovery (what it cost you to process the request). Also, you cannot charge a fee where the disclosure is required. At this time, no amount is prescribed under the regulation to PHIPA, O.Reg. 329/04.

CHAPTER 7

This chapter explains the process for clients to make formal written requests for access to and correction of their records of PHI. The access and correction rules under PHIPA apply to all health settings.

Access to and correction of records of personal health information

KEY POINTS

Access requests can be formal or informal.

If there is a formal written request for access, it falls under PHIPA and the client has certain rights. The custodian has numerous obligations, including responding in a certain way and within certain time frames.

Subject to limited and specific exceptions, the general rule is that your clients have a right of access to the records of personal health information (PHI) you hold about them.

A client may also ask to have a record of his/her PHI corrected. If the client can demonstrate that it is inaccurate or incomplete for the purpose for which you will use it, in most cases you must correct it.

However, you have the right to refuse to correct the record if it consists of a professional opinion made in good faith (yours or someone else's); or, if you did not create the record and lack the knowledge, expertise or authority to make the requested change.

Prescribed organizations will have similar responsibilities in responding to requests for access and correction of records of PHI. However, since it is not entirely clear as to how prescribed organizations will do so, you should continue to respond to requests for PHI that you have disclosed to the prescribed organization for electronic health records.

The client has specific rights under the access and correction rules, including the ability to attach a statement of disagreement to a record you refuse to correct, and to make a complaint to the Information and Privacy Commissioner in a number of circumstances.

Most custodians will develop processes to guide staff and clients about requests for access to, or correction of, a record of PHI (such as to whom within the agency an access request made by a client should be forwarded, how to give the types of notices and responses required by the Act, and how to apply the criteria for denial of access as set out in PHIPA).

PHIPA REFERENCE

For more complete information, you should also look at the following sections of PHIPA: 51-55

Formal versus informal requests

Nothing prevents you from giving access to, or making a correction requested by, a client in an informal way. For example, during a session with your client, you may decide to show him/her something in the health record. In that situation, though, a client is not entitled to all of the protections under the PHIPA rules.

Substitute decision-maker's right of access

A client's substitute decision-maker has the same right of access as the client.

Background on access

In 1992, following a dispute about a client's access to her health records held by a physician, the Supreme Court of Canada made an important decision about who owns a health record, and when people have the right to see what is in their records. Based on the facts of that case, the Supreme Court decided that the physician owned the actual record, but held it in trust for the individual whose information it contained. This case gave rise to a general right of people to access their health records, with certain exceptions. The court's ruling on ownership is a good way to think of the way you hold information on your client's behalf.

In keeping with that case, the starting point for the rules under PHIPA is that everyone has a right of access to his/her records of PHI, unless one of the exceptions under the Act applies. This means that a client may ask you for access to PHI that you have in your possession, including records of PHI that are held outside the traditional health record. If agency staff members have separate files or progress notes in their offices because they are working with a particular client, the client could ask to see those notes.

For example, a client may make a written request for access to a record of PHI held by a specific person, such as a drug counsellor who is working with a team to provide care to the client. A client could also ask for access to PHI held by specific individuals who work for your agency or in specific locations. You should work with the client to get a sense of what information he/she is really looking for.

PHIPA requires that if the client's request is too broad, you must assist the client to help you narrow it.

QUESTIONS AND ANSWERS

Q In the case of marital/family therapy, who does the record belong to?

A Information provided by an individual during marital or family therapy is accessible by that individual only, unless that individual consents to its release to others participating in the therapy. You should ensure that the method you use to record information does not prevent you from severing that information from other parts of the record.

Records to which the access rules do not apply

PHIPA sets out situations where an individual does not have a right to ask for certain records. The exclusions that may be applicable to your agency are

- PHI collected or created in order to comply with a health college's quality assurance program (which monitors the practices of all regulated health professionals such as physicians, nurses and occupational therapists),
- raw data from standardized psychological tests or assessments (most applicable to information generated by psychologists), and
- PHI that a custodian uses solely for research approved under PHIPA.

Denying the client's request for access to a record of PHI

A client has a general right to access his/her record of PHI. However, you must deny access to any part of a record where one or more of the following applies:

- You have reason to believe that giving the client access would interfere with any legal privilege attached to the record or information in the record
- The disclosure is prohibited by law or court order
- The information in the record was collected or created primarily in anticipation of, or for use in, a proceeding, and the proceeding, together with all appeals or processes resulting from it, have not been concluded
- All of the following conditions apply:

  (a) the information was collected or created in the course of an inspection, investigation or similar legally authorized procedure, or done in order to detect, monitor or prevent fraud and the inspection, investigation, or other procedure and any other appeals or processes have not been concluded

  (b) granting the access could reasonably be expected to:

    (i) result in a risk of serious harm to the treatment or recovery of the individual or a risk of serious bodily harm to any person

(ii) lead to the identification of a person who was legally required to give the information to the custodian, or

(c) the person who provided information in the record to the custodian did so in confidence and the custodian believes that person's identity should be protected

- Specific situations under municipal or provincial freedom of information legislation apply (which are not relevant to most mental health and addictions agencies and programs). However, the record of PHI may be disclosed to the institution to process a request under freedom of information legislation like the Freedom of Information and Protection of Privacy Act

You must remember to word your response very carefully, in order to meet the requirements of the Act. The following chart will guide you, and you can also refer to the four sample letters provided at the end of this chapter once you decide how you will answer your client's request.

It may be helpful as part of your access and correction procedures to make a clinician or someone else within your agency responsible for assessing whether any of the reasons above for denying the access request apply.

SITUATION	**YOUR RESPONSE**
You locate the record the client asked for. There is no reason to deny access to the record.	**Letter #1** – Make the record available to the client for examination, and if requested, provide a copy. If it is practical to do so, you should also explain any terms, codes, or abbreviations used in the record.
You look for but cannot find the record the client has asked for.	**Letter #2** – You must give the client written notice that, after a reasonable search, you have concluded that the record was not found or does not exist.
You locate the record the client asked for, but one of the exceptions to the right of access applies to all or part of the record.	**Letter #3** – You must give access to as much of the record as possible (which may include severing the part the client is not entitled to see).You must give the client written notice of the denial of access, and the reasons for the refusal. Cite the actual PHIPA provision, unless it is one of subsections 52(1)(c), (d) or (e); if it is, go to "Letter #4" below.

	Check to make sure that the reason for denial is not one that requires you to respond under "Letter #4" below.
You locate the record the client asked for, but one of the exceptions to the right of access applies to all or part of the record. You must deny access to any part or all of the record if you believe that giving it • would result in a risk of serious harm to the treatment or recovery of the client, or a risk of serious bodily harm to someone else, • would interfere with an inspection or investigation under a statute (such as the*Coroners Act*) and the matter is ongoing (including any appeals or other related processes) • would reveal the identity of someone who gave you the information in confidence, or • would lead to the identification of a person who was required by law to provide the information to you. You must also deny access if the information was collected/created for use in a court or other proceeding that is not yet finished (such as a court or tribunal hearing, mediation or arbitration).	**Letter #4** – You must give access to as much of the record as possible (which may include severing the part of the record the client is not entitled to see). You must also give the client written notice that you can neither confirm nor deny the existence of the requested records based on specific sections of PHIPA. You must **not** tell the client which section of PHIPA you are relying on, as this might escalate a situation that you are already concerned about (for example, harm to the client's treatment or recovery).

When you deny an access request to part or all of a record of PHI, you must do the following things:

- Sever the part of the record to which the client is not entitled, and provide the rest
- Inform the client of his/her right to make a complaint to the Information and Privacy Commissioner

When refusing, in addition to the above, you will provide one of the following three responses:

- You are refusing the request in whole or in part, while citing that the refusal is due to the fact that record was collected or created in anticipation of or for use in a proceeding; the record was collected or created in the course of an investigation, inspection or similar procedure authorized by law; or granting access could result in a risk of serious harm.
- You are refusing the request or whole in in part, but not citing the reasons.
- You are refusing to confirm or deny the existence of any record related to the grounds of refusal.

Timelines

You must respond to the client's request as soon as possible, and otherwise within 30 calendar days. You can only extend the time to 60 days if you need the extra time to locate the record or to consult about any reasons for denying the access request. If you extend the time beyond 30 days, you must first inform the client and give the reason for the extension.

A client can also ask that you respond to a request for access sooner than 30 days. If the client is able to demonstrate the urgency of the situation, you must fulfill the request if you are reasonably able to give the required response within that time period.

Fees

You may charge a fee for the access, but only if you first tell the client how much you think it will cost. Although there are no guidelines or regulations from the government to tell you what you should charge, PHIPA requires you to limit any fees to reasonable cost recovery (for example, what it cost you in staff time and photocopying costs to provide access). You should follow your agency's policies where they exist, and any applicable standards. For example, the College of Physicians and Surgeons of Ontario has a policy on medical records: http://www.cpso.on.ca/Policies-Publications/Policy/Medical-Records#29. In the section on fees, it cites reasonable cost recovery and the relevant footnote (#29) refers to the OMA Physicians Guide to Uninsured Services; PHIPA s 54(11) and IPC Order HO-009. This IPC Order speaks to

Denial on the basis of harm

You may be familiar with the concept of denying the client access to his/her record on the basis of serious harm to the treatment or recovery of the client, or serious harm to another person. A similar test was previously found in the Mental Health Act, but now appears in PHIPA.

Here are a few other changes you should keep in mind under PHIPA:

PHIPA & Denial of Access
A health information custodian who wishes to deny access does not need to go to the Consent and Capacity Board, but must inform the client of his/her right to make a complaint to the Information and Privacy Commissioner.
Access rules now apply to capable and incapable individuals, and to their substitute decision-makers.
You **may** consult a physician or psychologist to assist you in determining the risk of harm.
Time frame is as soon as possible, and no later than 30 days; you may extend to 60 days total if you give client notice and you need the time in order to locate the record or consult with others about the request.
Decision to deny is the custodian's; client can complain to the Information and Privacy Commissioner.

Correction of records

Once you have granted a client access to records of PHI, he/she may also ask that you make changes to those records. You must make the corrections if

- your client demonstrates that the record is incomplete or inaccurate for the purposes for which you use the PHI, and
- he/she gives you the information to make the correction.

However, you may choose not to make the corrections if,

- the PHI in question is a professional opinion made in good faith (either yours or someone else's; "professional" is not defined under PHIPA but generally could mean the opinion of anyone who has the authority to be charting the client's care — for example, a health care practitioner), or
- you did not originally create the record and you lack the knowledge, expertise or authority to make the correction.

Method of correction

The best method of correction is to strike out the incorrect information, but under no circumstances can you obliterate it. If it is not possible to strike out the incorrect information, you should consult PHIPA for other acceptable methods. If you are a health professional or are otherwise bound by certain professional standards, you need to consider those as well.

If you refuse to make a correction, you must tell your client of the right to make a complaint to the Information and Privacy Commissioner.

Timelines

The timelines for correction are the same as those for access: you must respond as soon as possible and no later than 30 calendar days. The exception is, if you require further time in order to locate the records or consult about correction, you can do so as long as you inform the client, and provide an updated timeline of up to 30 additional days. Note that if you exceed the 30 calendar days and do not provide that notice, you have committed what is called a ‘deemed refusal’. If you are organized, there is no reason to ever have a deemed refusal.

Fees

You cannot charge a fee for correction of a record.

QUESTIONS AND ANSWERS

Q A client disagrees with her diagnosis, and has asked that it be removed from her health record. Am I required to make the change?

A You can, but do not have to, change the record of PHI if the diagnosis was a professional opinion made in good faith; or if you didn't create the record and you lack the expertise, knowledge or authority within your agency to change or remove the diagnosis.

If you do make the correction, you must

- do it using an appropriate method (discussed above),
- notify the client that you have done so, and
- if the client requests it, give the corrected information to anyone to whom you previously gave the incorrect information (however, you do not have to do this if you believe that the correction would have no impact on the client's ongoing health care or interfere with some other benefit he/she may be entitled to).

If you choose not to make the correction, you must

- notify the client of the refusal,
- tell the client that he/she can prepare a short written "statement of disagreement" for you to attach to the record (setting out why the client believes the PHI is incorrect), and
- tell the client of his/her right to ask that you give the statement of disagreement to anyone to whom you had previously given the information the client is disputing.

However, even if a client asks, you do not have to give a copy of the statement of disagreement to others if you believe that there would be no impact on the client's ongoing health care or that it would not interfere with any benefits he/she might be entitled to.

TEMPLATES

TEMPLATE: ACCESS RESPONSE – Letter #1

Date

Name
Address
City, Province
Postal Code

1.

Re: Request for Access to Personal Health Information

Dear _____ :

I am writing in response to your recent request for access to your record of personal health information under the *Personal Health Information Protection Act,* which we received on *, 2005.

We have located the record you have asked for. Please call us at **[enter phone number]** to make an appointment to come in to review the record. Once you have had an opportunity to look at the record, you can also ask us for a copy of the record (and for information about the fee that may be charged for copies).

I would be happy to answer any questions you have.

Thank you for your request.

Yours truly,

TEMPLATE: ACCESS RESPONSE – Letter #2

Date

Name
Address
City, Province
Postal Code

Re: Request for Access to Personal Health Information

Dear _____ :

I am writing in response to your request for access to personal health information dated [date of request], which we received on [date request was received].

After a reasonable search, I can tell you that [choose one: no personal health information was found in the locations you have asked about OR we have concluded that the records you asked for do not exist]. We can make this statement based on s. 54(1)(b) of the Personal Health Information Protection Act (PHIPA).

I would be happy to answer any questions you have. You may also make a complaint about our response to the Information and Privacy Commissioner at:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Tel: (416) 326-3333

Toll-free: 1-800-387-0073

Thank you for your request.

Yours truly,

TEMPLATE: ACCESS RESPONSE – Letter #3

Date

Name
Address
City, Province
Postal Code

Re: Request for Access to Personal Health Information

Dear _____:

I am writing in response to your request for access to personal health information dated *, which we received on *, 2005.

I regret to tell you that your request has been denied under section 54(1) of the Personal Health Information Protection Act for the following reason:

[Cite any s. 54(1) provision other than s. 54(1)(c), (d) or (e)]

If you have any questions about this response, please contact me. You may also make a complaint about our response to the Information and Privacy Commissioner at:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Tel: (416) 326-3333
Toll-free: 1-800-387-0073

Thank you for your request.

Yours truly,

TEMPLATE: ACCESS RESPONSE – Letter #4

Date

Name
Address
City, Province
Postal Code

Re: Request for Access to Personal Health Information

Dear _____:

I am writing in response to your request for access to personal health information dated *, which we received on *, 2005. I can neither confirm nor deny the existence of the record you have requested, based on any of sections 54(1)(c), (d) or (e) of the Personal Health Information Protection Act.

[Attach all three sections: 54(1)(c), (d) and (e)]

I would be happy to answer any questions you have. You may also make a complaint about our response to the Information and Privacy Commissioner at:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Tel: (416) 326-3333
Toll-free: 1-800-387-0073

Thank you for your request.

Yours truly,

Q We have had numerous requests for access to, and correction of, records by a particular client. We are a small agency and are spending a lot of time on responding to these requests.

We want to be fair, but is there any way to stop any future requests?

A Clients are entitled to pursue their rights under PHIPA, and you should use reasonable efforts to make sure that this happens.

In rare situations, though, you may conclude that a client is not making requests in good faith. If you think that your client is making repeated requests just to annoy you or to overwhelm your agency's limited resources, you can refuse to respond to his/her requests for access or correction.

For the access request, you can simply not respond, and that lack of a response will be treated as a refusal. The client is free to make a complaint to the Information and Privacy Commissioner. In the

case of a request for correction, you must tell the client why you are not making the correction, and tell the client of his/her right to make a complaint to the Commissioner.

In both cases, the Commissioner will decide whether your position that the request is “frivolous,” “vexatious” or “made in bad faith” is legitimate.

You do need to be careful not to invade your client’s privacy (for example, you don’t necessarily have the right to ask specifically why the client wants access to the information).

Q During assessments, clients provide us with information about other

people (including family and friends). Do these family and friends have equal access to the client’s records?

A No. If the client provides information about family and friends, the information becomes part of the client’s record of PHI. It is not accessible by the family or friends (unless the family member or friend is the client’s substitute decision-maker).

CHAPTER 8

This chapter explains the main functions of your agency's contact person, often called the "Privacy Officer"; the Office of the Information and Privacy Commissioner of Ontario (Commissioner), which oversees compliance with PHIPA; and the Consent and Capacity Board (Board). It also gives you information about how your agency should handle complaints about your privacy practices, and what to expect if someone makes a complaint about you to the Commissioner.

The Privacy Officer, the Commissioner and the Board

KEY POINT

You should be familiar with the roles of the PHIPA contact person in your agency, the Information and Privacy Commissioner who oversees compliance with PHIPA, and the Consent and Capacity Board, which hears certain applications under the Act.

Privacy Officer

The Privacy Officer is the public face of privacy of your agency, and will answer questions about your privacy and information practices from clients and the public. The Privacy Officer is a resource to you, and should do his/her best to make sure that everyone in your agency is aware of their duties under PHIPA. He/she will also respond to and investigate any complaints about your privacy practices.

PHIPA does not give any guidance about how a Privacy Officer should handle complaints about your agency's privacy practices. Here are some suggested guidelines for your agency to follow if someone makes a complaint:

- If the complaint is made by way of a letter, send a written acknowledgement that the complaint has been received and when the person who complained can expect a reply.
- Open a file for each complaint that you receive.
- Investigate the complaint by speaking with those in your agency who are best able to give you information about the substance of the complaint.
- Assess whether the situation the person complained about is ongoing (even if it does not affect that person). If it is, take steps to rectify the situation.
- Provide a reply to the person who complained.

- Give a general notice to anyone involved in the investigation about how the matter was resolved.
- Prepare a summary of the incident in general terms to report to the senior management of the agency. To the extent possible, the summary should not divulge personal information about anyone involved in the complaint.
- Assess whether any steps should be taken to reinforce the importance of privacy and information protections within your agency (for example, training with a particular group of health care professionals, or the adoption of additional security safeguards).

The Privacy Officer should also be familiar with the rights a client has under PHIPA and when clients must be told about these rights or their ability to make a complaint to the Commissioner. A helpful list of issues that may be of concern to clients is provided in Chapter 9.

Breaches of PHIPA

If there is a breach of PHIPA, it is important that the Privacy Officer (or someone else in the agency) contact the person whose information has been lost, stolen, or accessed inappropriately. See Chapter 2 and 11 for more information about security safeguards and responding to breaches.

The Information and Privacy Commissioner

The Commissioner's role

Under PHIPA, the Information and Privacy Commissioner has a number of roles, including the following:

- To provide education and information to custodians, clients and the general public, as well as to hear the public's comments about PHIPA
- To oversee custodians' compliance with PHIPA
- To deal with complaints from clients and the public
- Upon request, to offer comments on a custodian's actual or proposed information practices
- To engage in or support research on matters related to PHIPA
- To assist his/her counterparts in other jurisdictions in their investigations (including the federal Privacy Commissioner)
- To conduct his/her own review of a custodian's practices

Commissioner's powers

The Commissioner has broad powers to investigate possible breaches of PHIPA. These include inspection and review powers, such as the ability to require a custodian to provide the Commissioner with documents and other materials, and the right to enter the custodian's premises (although a

warrant is required if the premises are also someone's home). Custodians must take care not to obstruct the Commissioner or the Commissioner's staff in these investigations.

Whistleblower protection

If someone complains about you to the Commissioner, or the Commissioner has any other reason to investigate your practices, the following information about the complaints process may be helpful:

- An intake analyst from the Commissioner's office will gather information about the complaint from the person who made it, and from you. This may be done in writing as well as by telephone. This may include questions about what steps the person who is complaining has taken, and the responses you have made, in the course of the complaint.
- The intake analyst will then prepare a report and ask both sides to review it. Throughout the process, the Commissioner's staff will attempt to have you and the person who complained settle the matter.
- The complaint may move on to "mediation." A mediator will also try to effect a settlement between the parties.
- If the complaint is not resolved at the mediation stage, it may move on to a Commissioner's review. However, the Commissioner may decide not to review a matter if:
    - the complaint could more appropriately have been dealt with through a different procedure,
    - the time between when the matter being complained about happened and the time the complaint was made is such that ruling on the matter would inappropriately prejudice someone,
    - the person complaining does not have a direct enough interest in the complaint, or
    - the complaint is frivolous, vexatious or made in bad faith.

For more information about the process, please see online:

https://www.ipc.on.ca/privacy/processing-privacy-complaints/

https://www.ipc.on.ca/health/phipa-complaint-process/simplifying-our-phipa-processes/

The Consent and Capacity Board

The Consent and Capacity Board is an independent body that conducts hearings under a number of laws, including PHIPA. Board members are psychiatrists, lawyers or members of the general public. The Board sits with one, three, or five members. Hearings are usually recorded in case a transcript is required.

The Board has the authority under PHIPA to

- review a finding of incapacity to consent to the collection, use or disclosure of PHI,
- consider the appointment of a representative for a person incapable to consent to the collection, use or disclosure of PHI, and
- review a substitute decision-maker's compliance with PHIPA's rules for substitute decision-making.

There are several forms under the Personal Health Information Protection Act that you should be aware of:

- Form P1 – Application to the Board to Review a Finding of Incapacity to Consent to the Collection, Use or Disclosure of Personal Health Information under Subsection 22(3) of the Act
- Form P2 – Application to the Board to Determine Compliance under Subsection 24(2) of the Act
- Form P3 – Application to the Board to Appoint a Representative under Subsection 27(1) of the Act
- Form P4 – Application to the Board to Appoint a Representative under Subsection 27(2) of the Act

These forms are available online at http://www.ccboard.on.ca/scripts/english/forms/index.asp.

CHAPTER 9

This chapter sets out some of the areas of PHIPA that may be of particular importance to clients. It also identifies when clients have the right under PHIPA to complain about a custodian to the Information and Privacy Commissioner.

PHIPA from your client's perspective

KEY POINTS

Clients like to be informed about specific issues (such as one's rights; substitute decision-making; access to one's health record; and specifics about what is sometimes referred to as a "lockbox").

You should also be familiar with the circumstances in which a client may make a complaint to the Information and Privacy Commissioner about your agency's privacy and information practices.

SELECTED CLIENT ISSUES

Topic	Rights information
PHIPA	When a health information custodian determines that a client is incapable to consent to the collection, use or disclosure of PHI, rights information may be provided if the custodian believes it is reasonable in the circumstances to do so.
Comment	Formal rights advice is mandatory in the community only when a physician is considering issuing a community treatment order, and the advice is provided to both clients and their substitute decision-makers, if any. Formal rights advice related to the collection, use or disclosure of PHI continues to be mandatory for clients of psychiatric facilities.

Topic	Automatic role of substitute decision-maker under HCCA for PHIPA information decisions related to treatment
PHIPA	An incapable client who has a substitute decision-maker under the *Health Care Consent Act* for treatment will have the same substitute decision-maker for information decisions that relate to the treatment.
Comment	This eliminates the need for health information custodians to find a new substitute decision-maker under PHIPA.

Topic	Determination of harm as basis of denying access to record now discretion of the custodian
PHIPA	A health information custodian may deny a client's access to a record of his/her PHI. There are rules about the types of responses a custodian must give, and for informing the client of the right to make a complaint about the response to the Information and Privacy Commissioner. The custodian has the right but no obligation to consult with a physician or psychologist prior to denying access on that basis.
Comment	Under the former *Mental Health Act* rules, the attending physician in a psychiatric facility who wished to withhold a patient's clinical record had to apply to the Consent and Capacity Board for permission to do so.

Topic	Timeframes for custodians to respond to access and correction requests now up to 60 days (previously 7 days)
PHIPA	PHIPA has set timeframes in which you must respond to a client's request for access to, or correction of, his/her record of PHI.
Comment	Anyone who has ever been a patient in a psychiatric facility may raise the fact that access requests were answered within 7 days under the *Mental Health Act*. You may want to inform your clients when they make a request for access, or correction, of the new time frames under PHIPA, and that the rules apply in all health settings (including psychiatric facilities).

Topic	"Lockbox" and its limitations
PHIPA	Clients may instruct a custodian not to use or disclose their PHI in particular circumstances (mainly relating to health care purposes).
Comment	Lockbox is limited in its scope. It cannot be used by clients to stop a custodian from using or disclosing PHI if the Act permits or requires the custodian to do so.

Topic	Consent to have the custodian leave a copy of the client's record of PHI in the client's home or someplace else.
PHIPA	A health information custodian may leave a record of the client's PHI in the client's home or in another location not under the custodian's control in certain circumstances.
Comment	Clients should consider their own ability to safeguard the record of PHI, and who may have access to it.

What can a client do under PHIPA?

A client has many rights under PHIPA, including the right to

- withdraw or withhold his/her express or implied consent for collection (including indirect collection), use or disclosure of PHI,
- request access to or correction of a record of PHI, or to attach a statement of disagreement,
- request a fee waiver for access to a record of his/her PHI,
- instruct the custodian not to use his/her PHI or to disclose it to other custodians for health care purposes
- ask a custodian for a copy of its written public statement (which includes a description of the custodian's information practices; who the contact person is for the custodian and how to reach him or her; and how to make a complaint to the Information and Privacy Commissioner),
- ask for your help in narrowing an access request, and
- make different types of complaints to the Information and Privacy Commissioner.

CHAPTER 10

This chapter provides an overview of the framework for electronic health records. It provides a general understanding of how prescribed organizations (such as eHealth Ontario) will develop and maintain PHI in the provincial electronic health record (EHR). As well, PHIPA governs how custodians collect, use and disclose PHI in the context of this provincial EHR.

Electronic Health Record

Key Points

- Bill 119 has amended PHIPA to include Part V.I which creates a framework for the provincial EHR. At the date of this publication, Part V.I has not been proclaimed in force and no related regulations have been released.

PHIPA Reference

For more complete information, see Part V.I of PHIPA: 55.1

Who are the Prescribed Organizations from which PHI may be collected, used or disclosed?

Prescribed organizations will be designated in the regulations, and have certain responsibilities and obligations in overseeing the EHR.

What are the Prescribed Organizations' Responsibilities?

Prescribed organizations have certain responsibilities and obligations to oversee the provincial EHR. They will collect PHI from custodians to be included in the EHR. Some of their responsibilities include:

- Manage and integrate PHI it receives from you.
- Ensure EHR functions properly by servicing the electronic systems.
- Conduct data quality assurance activities to ensure accuracy and quality of PHI.
- Analyze PHI to provide alerts and reminders to custodians in their provision of health care.
- Log, audit and monitor instances where PHI is viewed, handled or otherwise dealt with, and where consent directives are made, withdrawn, modified and overridden. As a custodian, you

may ask for these electronic records in order to audit and monitor your compliance under PHIPA.
- Have and comply with practices and procedures that are approved by Information and Privacy Commissioner of Ontario every three years.

Prescribed organizations also have to comply with certain requirements in developing and maintaining the PHI such as ensuring that the PHI it receives is reasonably necessary for the purposes of EHR, and protected from unauthorized collection, use, and disclosure. As a custodian, you can expect the prescribed organizations to provide the following to you:

- Plain language description of the EHR, and its administrative, technical, and physical safeguards.
- Any directives, guidelines and policies as it relates to the EHR.
- Written copy of results of the assessments for each system that retrieves, processes, or integrates PHI.
- If there is a privacy breach, you must be notified at the earliest opportunity. You are then responsible for notifying individuals at the first reasonable opportunity if PHI in your custody or control is stolen, lost or used or disclosed without authority. You must also notify the Commissioner if the circumstances surrounding theft, loss, or unauthorized collection, use or disclosure meet certain requirements (not yet prescribed)

A year after Part V.I is proclaimed into force, the prescribed organizations will have to have procedures and policies developed for purpose of protecting the privacy and confidentiality of PHI in the EHR. Special rules for collecting, using and disclosing in the context of EHR?

Special definitions of collection, use and disclosure will apply in the context of the EHR:

Collection

- A collection is when for the first time, you view, handle, or deal with all or part of PHI in the EHR, which was provided by another custodian to the prescribed organization. This is considered a collection. If you subsequently view, handle, or otherwise deal with the PHI in the EHR, it is considered a use.
- In general, custodians will only be permitted to collect PHI from the provincial EHR to provide or assist in the provision of health care to the individual or if the custodian has reasonable grounds to believe it is necessary to eliminate or reduce significant risk of seriously bodily harm.
- It is also important to remember that if PHI is collected to provide health care, it may only be used or disclosed for any purpose permitted by PHIPA. Secondly, if there is significant bodily harm, the PHI collected may be used and disclosed only for this purpose.

Use

- It is also a use of PHI when you view, handle or otherwise deal with (e.g. printing, scanning, uploading) all or part of the PHI in the EHR that you provided to the prescribed organization.

Disclosure

- A disclosure is when the PHI you provided to a prescribed organization is collected by another health information custodian. However, when you are simply disclosing PHI to the prescribed organization for inclusion of the EHR, it is not considered a disclosure.

What are your obligations as a custodian?

As a custodian viewing and/or contributing to the provincial EHR, you can only collect PHI in two circumstances:

1. To provide health care (or to assist in providing health care) to an individual to which the PHI relates; or

2. To reduce or eliminate a significant risk of serious bodily harm to a person (the client or a third party), or a group of persons, and you have reasonable grounds to believe the collection is necessary to address this risk.

You are allowed to collect, use, and disclose any of the data elements set out in the regulation for the purpose of uniquely identifying an individual.

As a custodian, you are already required to protect the PHI you hold. Similar rules apply here: you must protect PHI you receive from the prescribed organization. Specifically, you must protect such PHI from theft, loss, and unauthorized use, disclosure, copying, modification or disposal. In the event of unauthorized use, disclosure, or collection, you must also notify the individual and, if the circumstances meet the prescribed requirements (not yet set out), the Information and Privacy Commissioner.

How do consent directives work in the EHR Context?

As discussed in Chapter 3, 5, and 6, individuals have the right to withhold or withdraw their consent for the collection, use, or disclosure of PHI in certain situations. This is informally referred to as a “lockbox”.

In the context of the provincial EHR, an individual can submit a consent directive to the prescribed organization to withdraw or modify their consent. If a custodian requests PHI that is subject to a consent directive, the prescribed organization will notify the custodian and provide only the PHI that is not subject to the directive.

There are exceptions to this rule. Even if an individual has put in place a consent directive, the original custodian of the PHI can disclose PHI to another custodian in these ways:

1. With the express consent of the individual is obtained; or

2. There are reasonable grounds to believe that the collection is necessary to reduce or eliminate a significant risk of serious bodily harm to the individual or one or more other individuals, and it is not reasonable in the circumstances to obtain the individual's consent.

As well, in these scenarios, you can only use the PHI for the purpose for which it was collected.

It is also important to note that when a consent directive is overridden, the prescribed organization is required to immediately provide written notice to the custodian that collected the PHI.

Upon receipt of such notice, as a custodian, you will be required to do the following:

1. Notify the individual to whom the PHI relates at the first reasonable opportunity; and

2. Where PHI is collected to eliminate or reduce a significant risk of seriously bodily harm to a third person, provide written notice to the Commissioner.

CHAPTER 11

This chapter provides an overview of what constitutes unauthorized collection, use, and disclosure of PHI. In recent years, there has been a rise in the number of cases where workers in the health care setting have been prosecuted for snooping in health records of patients they do not provide care for. We will discuss what constitutes as a privacy breach, and your obligations and responsibilities under PHIPA when a breach occurs.

Privacy Breaches

Key Points

- A use of PHI is defined as viewing, handling, or otherwise dealing with the information. In the past, “view” was not part of the definition of PHI under PHIPA, but in light of recent privacy breaches, it is an important component of what is considered now as a “use” of PHI.
- In the event of a privacy breach, there is an obligation to notify the affected individual at the first reasonable opportunity and if the situation meets the prescribed requirements, notifying the Information and Privacy Commissioner (these requirements have not been prescribed yet).
- In the context of the provincial EHR, the custodian must also notify the individual at the first reasonable opportunity if PHI is collected without authority.
- There is also an obligation to notify your employee’s regulatory college in circumstances where their termination, resignation, and discipline is due to unauthorized collection, use, disclosure, retention or disposal of PHI.
- Fines of a maximum of $100,000 for individuals and a maximum of $500,000 for corporations.
- There is no limitation period for prosecution under PHIPA.

PHIPA Reference

For more complete information, you should also look at sections 12 and 17.

What is a Privacy Breach?

A privacy breach is when the PHI in the custodian's control or custody is stolen, lost, or there is unauthorized use, or disclosure. This includes unauthorized copying, modification, or disposal. It also includes viewing PHI that one does not have authority to view, i.e., "snooping".

Background

In recent years, there have been numerous cases involving workers in the healthcare industry snooping records for purposes (i.e. curiosity, jealousy) other than for the purpose of providing healthcare to the patient. For example, in Hopkins v Kay, 280 patient records were improperly accessed by hospital employees and then disclosed to third parties.

This issue hasn't only plagued the health care sector, but has become such an issue that the Information and Privacy Commissioner launched a new campaign "Is it Worth It?" to educate the public against snooping. You can read more about the resources provided by the Information and Privacy Commissioner here: https://www.ipc.on.ca/health/unauthorized-access/

Notification to the Individual, IPC and College

You must ensure that the PHI that is in your custody or control is protected against theft, loss, unauthorized use, or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification, or disposal. In the event there is a privacy breach involving the PHI, you must notify the individual and also tell them that they have the right to complain to the Information and Privacy Commissioner.

Secondly, if the circumstances of the breach meet the prescribed requirements (not yet set out in the regulations), you must notify the Information and Privacy Commissioner as well.

Until the regulations give more detail about what must be reported, it is important you take a more conservative approach in dealing with any privacy breaches in the interim (i.e. informing the Information and Privacy Commissioner). If you are unsure, it is always better to contact the Information and Privacy Commissioner and/or to seek legal assistance.

Notice to a Regulatory College Governing Health Care Professional

In the event you employ a health care practitioner who has committed a privacy breach, you must notify the college that regulates their health profession. A college means a college that oversees a member of health profession that is regulated under the Regulated Health Professions Act (RHPA) which includes the following:

- Audiology and speech-language Pathology
- Chiropody
- Chiropractic

- Dental Hygiene
- Dental Technology
- Dentistry
- Denturism
- Dietetics
- Homeopathy
- Kinesiology
- Massage Therapy
- Medical Laboratory Technology
- Medical Radiation Technology
- Medicine
- Midwifery
- Naturopathy
- Nursing
- Occupational Therapy
- Opticianry
- Optometry
- Pharmacy
- Physiotherapy
- Psychology
- Psychotherapy
- Respiratory Therapy
- Traditional Chinese Medicine

A college would also include the Ontario College of Social Workers and Social Service Workers.

As a custodian, you must provide written notice to the college within 30 days in the following situations:

1. Employee is terminated, suspended, or subject to disciplinary action as a result of an alleged unauthorized collection, use, disclosure, retention, or disposal of PHI by the employee.
2. Employee resigns and you have reasonably grounds to believe it was because of an investigation or other action by the custodian with respect to the alleged unauthorized collection, use, disclosure, retention, or disposal of PHI by the employee.

In the case, where you grant privileges of (typically in the context of the Public Hospitals Act) or are affiliated with a health care practitioner who is a member of a college, you must provide written notice within 30 days of the event occurring to the college in the following situations:

1. The employee's membership privileges or affiliation are revoked, suspended, restricted as a result of the unauthorized collection, use, disclosure, retention, or disposal of PHI by the employee.
2. The employee relinquishes or voluntarily restricts his/her privileges or affiliation and you have reasonable grounds to believe that the relinquishment is due to an investigation or other means of action with respect to the alleged unauthorized collection, use, disclosure, retention, or disposal of PHI by the employee.

This notification requirement to the colleges would also extend to agents of the custodian.

Consequences of a Privacy Breach

We have already touched upon the consequences of not complying with PHIPA in Chapter 2. There is also no limitation period to prosecution that is brought under PHIPA, and the consent of the Attorney General must be obtained before prosecution can begin. These same principles would apply for a privacy breach.

If you are found guilty of unauthorized collection, use or disclosure under PHIPA, you can be fined up to $100,000 (for individuals) or $500,000 (for corporations).

Traditionally, Ontario law did not recognize the tort of breach of privacy, but that changed in a precedent setting case where a bank employee outside the health sector improperly accessed another bank employee's electronic banking records for several years. Her motive for doing so was personal in nature as she was in a relationship with the bank employee's former husband. The affected employee brought an action under the court systems and the Ontario Court of Appeal established this new cause of action in tort called the "intrusion upon seclusion".

In *Hopkins v Kay*, the Ontario Court of Appeal also ruled that individuals can pursue civil action and remedies outside of PHIPA. Custodians are at risk of being liable for more substantive damages outside of PHIPA.

Custodians can also be subject to class actions lawsuits. In Newfoundland and Labrador, a hospital employee was found, through an internal audit, to have accessed 1043 patients' health records without authorization. This has resulted in a civil action by the plaintiffs seeking damages from the hospital and it was certified into a class action by the courts. Besides the monetary consequences of not adhering to PHIPA, there are many other non-monetary consequences to consider.

There are reputational risks, which can negatively affect the public's perception and trust in your abilities to adequately safeguard their PHI against privacy breaches. It will not only affect your patient's trust in your abilities to protect their privacy, but also in your abilities as a health care provider. This is something that cannot be taken light-heartedly, as a patient's trust is key to providing health care.

It is imperative that you have robust risk management and privacy policies and procedures in place to prevent and mitigate any privacy breaches. For example, setting out a procedure laying out the proper steps in how to manage and address a privacy breach. You must also provide ongoing annual training to your staff to educate them on what constitutes as unauthorized collection, use and disclosure.

Questions and Answers

Q My colleague is providing community services to my uncle. Since I work at the same health care agency, can I use my employee access to view my uncle's health records to know more about his treatment?

A No. We understand that you are concerned about your uncle. However, this is considered unauthorized use of the PHI contained in the health records. You are viewing the files with the intentions to learn more about your uncle's treatment, when you do not have permission to access those records as you are not the service provider for your uncle; and you do not have his consent. If your uncle (or if he is incapable, his substitute decision-maker) consent to give you access, you must go through the agency's usual processes.

Glossary

Agent means a person that, with the custodian's authority, acts for or on behalf of the custodian with respect to personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being paid.

Capable means mentally capable.

Collect means to gather, acquire, receive or obtain personal health information by any means from any source.

College means a college that oversees a member of a health profession regulated under the Regulated Health Professions Act, 1991, and also includes the Ontario College of Social Workers and Social Service Workers.

Custodian. See definition for "health information custodian."

Disclose, in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person (this is different than a use of the information within your agency).

Electronic Health Record means the electronic system that were developed and maintained by the Prescribed Organizations for the purpose of enabling health information custodians to collect, use and disclose the PHI.

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

(a) is carried out or provided to diagnose, treat or maintain an individual's physical or mental condition,
(b) is carried out or provided to prevent disease or injury or to promote health, or
(c) is carried out or provided as part of palliative care, and includes,
(d) the compounding, dispensing or selling of a drug, a device, equipment or any other item to an individual, or for the use of an individual, pursuant to a prescription, and

(e) a community service that is described in subsection 2 (3) of the *Long-Term Care Act, 1994* and provided by a service provider within the meaning of that Act.

Health care practitioner means

(a) a person who is a member within the meaning of the Regulated Health Professions Act, 1991 and who provides health care,
(b) a person who is a member of the Ontario College of Social Workers and Social Service Workers and who provides health care, or
(c) any other person whose primary function is to provide health care for payment.

Health information custodian means a person or organization who has custody or control of personal health information as a result of their duties as follows:

1. A health care practitioner or a person who operates a group practice of health care practitioners
2. A service provider within the meaning of the *Home Care and Community Services Act, 1994* who provides a community service to which that Act applies
3. A community care access corporation within the meaning of the Community Care Access Corporations Act, 2001
4. A person who operates one of the following facilities, programs or services:
    (i) A hospital within the meaning of the Public Hospitals Act, a private hospital within the meaning of the Private Hospitals Act, a psychiatric facility within the meaning of the Mental Health Act, or an independent health facility within the meaning of the Independent Health Facilities Act
    (ii) A long-term care home within the meaning of the Long-Term Cares Home Act, 2007, a placement co-ordinator described in subsection 40(1) of that Act, or a care home within the meaning of the Residential Tenancies Act, 2006
    (iii) A retirement home within the meaning of the Retirement Homes Act, 2010
    (iv) A pharmacy within the meaning of Part VI of the Drug and Pharmacies Regulation Act
    (v) A laboratory or a specimen collection centre as defined in section 5 of the Laboratory and Specimen Collection Centre Licensing Act
    (vi) An ambulance service within the meaning of the Ambulance Act
    (vii) A home for special care within the meaning of the Homes for Special Care Act
    (viii) A centre, program or service for community health or mental health whose primary purpose is the provision of health care.
5. An evaluator within the meaning of the *Health Care Consent Act, 1996* or an assessor within the meaning of the *Substitute Decisions Act, 1992*
6. A medical officer of health of a board of health within the meaning of the Health Protection and Promotion Act
7. The Minister of Health and Long Term Care, together with the Ministry if the context so requires

8. Any other person prescribed as a health information custodian if the person has custody or control of personal health information as a result of or in connection with performing prescribed powers, duties or work or any prescribed class of such persons.

Health information network provider means a person who provides services to two or more health information custodians where the services are provided primarily to custodians 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.

Identifying information means information that identifies an individual, or for which it is reasonably foreseeable under the circumstances that it could be utilized, either alone or with other information, to identify an individual.

Incapable means mentally incapable.

Information practices means the policy of the custodian for actions in relation to personal health information, including

(a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
(b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information.

Mixed records means a record that includes both personal health information and non-personal health information (once it is a mixed record the whole record should be treated as a record of PHI under PHIPA).

Personal health information (PHI) means identifying information about an individual in oral or recorded form, if the information

(a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
(c) is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual,
(d) relates to payments or eligibility for health care,
(e) in respect of the individual,
(f) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
(g) is the individual's health number, or
(h) identifies an individual's substitute decision-maker.

Note: There are exceptions to what is considered personal health information under PHIPA, including when

(a) the identifying information contained in the record relates primarily to one or more employees or other agents of the custodian, and
(b) the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents.

Prescribed Organization is the organization or organizations that are prescribed by the regulation for the purposes of electronic health record (EHR).

Proceeding includes a proceeding held in, before or under the rules of a court, a tribunal, a commission, a justice of the peace, a coroner, a committee of a college within the meaning of the Regulated Health Professions Act, 1991, a committee of the Board of Regents continued under the Drugless Practitioners Act, a committee of the Ontario College of Social Workers and Social Service Workers under the Social Work and Social Service Work Act, 1998, an arbitrator or a mediator.

Privacy Officer is the contact person under PHIPA your agency has designated to answer questions from clients and the public about your privacy and information practices. For more information, see Chapter 8.

Record means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record.

Research means a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research.

Use in relation to personal health information in the custody or under the control of a health information custodian or a person, means to view, handle or otherwise deal with the information, but does not include to disclose the information. Sharing of PHI between a custodian and the custodian’s agent is a use of PHI, not a disclosure.

Related Links

Community Mental Health and Addictions Privacy Toolkit

www.privacytoolkit.ca

The complete Privacy Toolkit is available online. Visit the website for updates, downloadable templates, and more.

Consent and Capacity Board

www.ccboard.on.ca

E-Laws of Ontario

https://www.ontario.ca/laws

The e-Law website provides consolidated laws of Ontario. Please visit this site for applicable Ontario legislation such as PHIPA.

Information and Privacy Commissioner of Ontario

www.ipc.on.ca

The IPC website is a resource to obtain factsheets, orders and decisions. There is always new material on the site and you should visit it regularly to keep up-to-date with current privacy developments.

There are factsheets that might be helpful to you and your organization. The factsheets discuss topics such as:

- safeguarding PHI
- understanding access and correction rights
- lockbox
- encrypting information on mobile devices
- obtaining PHI from a deceased relative
- secure transfer of PHI
- protecting against ransomware

There are also orders and decisions related to other topics, including:

- snooping
- mobile devices and new technology
- access and correction
- closing a practice
- disclosing records of deceased

Personal Health Information Protection Act, 2004

https://www.ontario.ca/laws/statute/04p03/v2

PHIPA Regulations (O. Reg. 329/04)

https://www.ontario.ca/laws/regulation/040329