Advice to the Profession: Protecting Personal Health Information

Advice to the Profession companion documents are intended to provide physicians with additional information and general advice in order to support their understanding and implementation of the expectations set out in policies. They may also identify some additional best practices regarding specific practice issues.

Protecting patients' personal health information (PHI) is fundamental to providing high quality patient care. To establish and preserve trust in the physician-patient relationship, patients must be confident that their PHI is protected. This Advice document is intended to help physicians interpret and understand the legal and professional obligations to protect patients' PHI. If you are uncertain about how to discharge any of these obligations in specific circumstances, you are advised to consult the Canadian Medical Protective Association (CMPA), your legal counsel, or the Information and Privacy Commissioner (IPC).

General Principles

What is the difference between confidentiality and privacy?

Patients' PHI is protected when it remains confidential and private. Physicians are generally familiar with the duty of confidentiality, which prohibits them from sharing information about a patient without the patient's consent, unless permitted or required by law. In contrast, the duty of privacy is broader and prohibits physicians from accessing PHI where they have no authority to do so. At its essence, it is the difference between "don't share" and "don't even look!"[1]

These principles are reflected in the *Personal Health Information Protection Act, 2004* (*PHIPA*), which sets out a framework for when health information custodians and their agents, including physicians, are authorized to collect, use, and disclose PHI. While the legislation is complex, its general principles impose an obligation on physicians to only access PHI on a "need to know" basis, or where otherwise permitted or required by law to do so.

What is "snooping"?

Snooping is when a health care provider accesses a patient's PHI without authorization – in other words, when they have no need to know as part of their duties, and are not otherwise permitted or required by law to access the PHI.

[1] Kate Dewhirst, "New snooping case for health privacy – Decision 74 of the IPC released," September 5, 2018.

Some health care providers mistakenly believe that they are permitted to review a patient's PHI so long as they maintain the patient's confidentiality by not sharing it with anyone else. In reality, snooping is a breach of patient privacy. Unless authorized by law, physicians must have the patient's express consent to access the PHI where they do not need it to provide health care.[2] So, for example, physicians with technical sign-in ability may be snooping if they view health records where they have no need to know to provide care to the patient; the authority to sign in to an Electronic Health Record or Electronic Medical Record is not authority to access all or any records in the system.

PHIPA refers to "health information custodians" and "agents". What are these?

A "health information custodian" ("custodian") is a person or organization who, as a result of their power, duties, or work, has custody or control of PHI. This includes health care organizations such as hospitals, pharmacies, and laboratories, as well as some individual physicians (such as owners of a clinic, physicians working as a sole practitioner in their own practice) and some Family Health Organizations.[3]

In contrast, an "agent" is a person who is authorized by a custodian to perform certain activities on its behalf regarding PHI. Generally speaking, this includes physicians practising in hospitals and certain medical clinics. Administrative staff in a medical clinic or hospital may also be agents.

Agents may collect, use, or disclose PHI only as authorized and directed by their custodian. Custodians may permit their agents to collect, use, or disclose PHI only in certain circumstances, including if this is necessary for the agents to carry out their duties. Custodians are ultimately responsible for PHI, as well as the actions of their agents.

While *PHIPA's* framework is complex, custodians and agents are ultimately obliged to meet the same general expectations regarding the collection, use, and disclosure of PHI. The expectations in the policy therefore apply to *all* physicians, regardless of whether they are a custodian or an agent, as does the guidance in this Advice unless noted otherwise.

However, if you are a custodian, you should be aware of additional *PHIPA* rules that apply specifically to custodians, such as those regulating the retention, transfer, and destruction of records. If you are a custodian, you are advised to consult *PHIPA* and the CPSO's *Medical Records Stewardship* [hyperlink] policy for further information regarding these obligations.

[2] Where express consent is required, you are advised to document it in the patient's medical record, either by including a paper copy of the consent form (where the consent is given in writing) or a record of the conversation (where the consent is given orally).

[3] This list is non-exhaustive; a full legislative definition, along with certain exceptions, is found s. 3 of *PHIPA*.

Who is found within the "circle of care"?

The term "circle of care" is not found in *PHIPA*, but is commonly used to determine whether a physician can rely upon implied consent to access and share PHI. The circle of care is made up of health care providers who need access to the patient's PHI in order to provide the patient with health care. The IPC document, *Frequently Asked Questions: Personal Health Information Protection Act* provides the following examples of who is within the circle of care:

- In an office setting, the circle of care may include the physician, a nurse, a specialist or other health care practitioner referred by the physician, and any other health care practitioner selected by the patient, such as a pharmacist or physiotherapist.
- In a hospital setting, the circle of care may include the attending physician and the health care team (residents, nurses, clinical clerks and employees assigned to the patient with the responsibility of providing care to the patient). The circle of care could include a person outside the hospital who will be involved in providing health care to the patient upon discharge from the hospital.

The circle of care does *not* include:

- Health care providers who are not part of the direct or follow-up treatment of a patient, as these individuals do not need the PHI to provide health care to the patient; and
- Non-health care providers, like family, friends, the police, an insurance company, and the patient's employer.

When does the circle of care begin and end?

PHIPA does not address timing with respect to when a physician formally enters or exits the circle of care. Determining if you are within the circle of case will be an assessment based on the role you are playing in the patient's care.

As an example, if you have provided the patient with treatment and are continuing to provide follow-up care to the patient, you are still within the circle of care and may assume you have implied consent to access their PHI to provide health care to the patient. However, a physician does not necessarily continue to be in a patient's circle of care indefinitely. If you are not directly providing health care and/or follow-up treatment, you may no longer have the right to rely on implied consent to access the patient's PHI.

When in doubt, check with your custodian (e.g., hospital) or the IPC to find out if you are permitted to access the patient's PHI.

Am I snooping if I access a patient's PHI for education or quality improvement purposes?

It is common for physicians to want to access a patient's PHI in order to understand and assess the outcome of their treatment decisions, and *PHIPA* permits this kind of activity in certain circumstances.

For example, a custodian may permit its agents to use PHI without consent for limited secondary purposes. These purposes include:

- Education, such as where cases are reviewed with trainees and/or presented during rounds (though keep in mind that PHI should not be used where other non-identifying information will meet the purpose); and
- Risk management, error management, and quality improvement, such as where patient outcomes are reviewed to evaluate the effectiveness of personal practice or programs.

If your custodian permits its agents (physicians) to access PHI for these purposes, you can do so without consent of the patient to meet the purpose, subject to any restrictions or conditions imposed by the custodian. If your custodian has not expressly permitted its agents to access PHI for these purposes, you may not do so. You should therefore exercise caution and determine whether you have proper authority to access a patient's PHI in these situations – and when in doubt, check with your custodian to find out if you are permitted to do so.

If you are a custodian, *PHIPA* also permits you to disclose a patient's PHI to certain other custodians where:

- you and the other custodian have both provided health care to the same patient; and
- you are disclosing the PHI to improve or maintain the quality of care you have provided to that patient or to other patients receiving similar health care.

These rules permit custodians to discuss with each other the treatment and outcomes of care they have provided to a patient. For further information you may wish to refer to s. 39(1)(d) of *PHIPA*.

In any of the above circumstances, keep in mind that accessing information about a patient's condition or outcome simply out of interest is *never* permitted under *PHIPA*.

What do I do if non-emergency treatment cannot be safely provided because of the existence of a lockbox?

Where safe care cannot be provided due to the existence of a lockbox, the patient must be told the reason why they cannot receive (or continue to receive) the care and treatment they seek. The purpose of this discussion is to promote clear communication between the patient and

physician, and to ensure that the patient has an informed understanding of the implications of their decision to create the lockbox. This conversation may also provide an opportunity to revisit the existence of the lockbox with the patient and to seek their express consent to access the locked information for the purpose of the treatment.

Permitted and Required Disclosures

In what situations am I permitted to disclose PHI without consent?

In some circumstances, *PHIPA* permits physicians to disclose PHI without consent. These include disclosures relating to:

- **Assisting in a police investigation.** You are advised to consult legal counsel and/or the CMPA in these circumstances.
- **Eliminating or reducing significant risk of serious harm** to a person or group of persons. You are advised to document all activities in this respect in the patient's medical record.
- **Facilitating health care under exceptional circumstances**. If the disclosure is reasonably necessary for the provision of health care and it is not reasonably possible to obtain the patient's consent in a timely manner – for example, in an emergency situation where the patient is not capable of consenting and an SDM is not readily available – you are permitted to disclose relevant information to other physicians and certain other health professionals.
- **Reporting physician (or other health care provider) incapacity and incompetence**, where this is appropriate in the circumstances.
- **Regulating the medical profession**. You are permitted to disclose PHI to the CPSO for the purpose of administering and enforcing the *RHPA, 1991*, including carrying out regulatory duties such as investigations and assessments.
- **A proceeding or contemplated proceeding** in which you or your hospital is, or is expected to be, a party or witness.

This list is not exhaustive; please refer to sections 38-50 of *PHIPA* and the CPSO's *Mandatory and Permissive Reporting* policy for further information.

In what situations am I required to disclose PHI without consent?

In some circumstances, you are required by the law to disclose a patient's PHI, regardless of whether the patient consents. While not an exhaustive list, the following examples provide an overview of the circumstances you might encounter most frequently:

- **Mandatory reports** listed in the CPSO's policy on *Mandatory and Permissive Reporting*, including reports of suspected impaired driving ability under the *Highway Traffic Act* and reports to the Ontario Coroner under the *Vital Statistics Act* and the *Coroners Act*.
- **Disclosures required by the Ministry of Health and Long-Term Care** in order to monitor or verify claims for payment for health care, or for goods used for health care that are funded by the Ministry.
- **Reports required by the Workplace Safety and Insurance Board** in circumstances where health care is being provided to a worker claiming benefits under their workplace insurance plan.
- **Critical incident reports**, as required by the "Hospital Management" regulation[4] under the *Public Hospitals Act*.
- **Search warrants** (which grant the police broad authority to search for and seize evidence, including records) and **court summons** (which may require you to attend court with specific documents or materials). In these cases, you are advised to consult legal counsel and/or the CMPA, including their resources on physician interactions with police.

What do I do in the event of a privacy breach?

A "privacy breach" refers to a theft, loss, or unauthorized access, use, or disclosure of PHI that contravenes *PHIPA*. Reporting privacy breaches is the responsibility of custodians. In particular, custodians are required to notify the affected individuals of a privacy breach at the first reasonable opportunity. This notice is required by *PHIPA* to include a statement that the individual is entitled to make a complaint to the IPC under Part VI of PHIPA. Custodians are also required to report certain privacy breaches to the IPC, including where:

- PHI was stolen, lost or used or disclosed without authorization;
- there is reason to believe, after an initial privacy breach, that the PHI will be further used or disclosed without authorization;
- the breach is part of a pattern;
- the breach relates to a disciplinary action against a health profession college or non-college member; or
- the breach is significant, having regard to the circumstances, including the sensitivity, volume, and scope of the PHI involved.

In addition to notification of individual privacy breaches, custodians also required by *PHIPA* regulation to track and annually report to the IPC the number of times PHI was stolen, lost, or accessed, used, or disclosed without authorization in the previous calendar year. The annual

[4] R.R.O. 1990, Reg. 965.

reporting requirement applies to all breaches, not just those that meet the above criteria for individual notice.

For further information about privacy breaches, and what to include in notices and the annual report to the IPC, see the CPSO's *Mandatory and Permissive Reporting* policy, the IPC document *Responding to a Health Privacy Breach: Guidelines for the Health Sector*, and the *PHIPA* and its regulation.

Requests for Information from Third Parties: Friends, Family, and Research

This section deals with requests for patient information from third parties. In all of the following scenarios, the general rules under *PHIPA* apply: unless otherwise permitted or required by law, PHI can only be shared with third parties with the express consent of the patient.

What do I do if a friend or family member, who is not the patient's SDM, requests access to the patient's medical information or records?

It is not uncommon for physicians to be asked by a family member or friend about the condition of a patient or for information about the patient's health, and these situations can be challenging to manage. Where you cannot obtain the patient's consent to disclose their PHI, you may be permitted to do so by law where the disclosure is required to:

- contact a relative, friend, or potential SDM if the patient is injured, incapacitated, or ill and unable to give consent personally; or
- eliminate or reduce a significant risk of serious bodily harm to a person or group of persons, including the patient.

In addition, where the patient is deceased, *PHIPA* allows you to disclose PHI in order to:

- identify the patient;
- advise of the patient's death and the circumstances of death; and
- provide information that relates to the patient where it is needed by a spouse, partner, sibling, or child to make health care decisions.

When managing a request for information from family or friends, use your professional judgment and limit disclosure about the patient's state of health unless one of the above circumstances applies.

What do I do if a child patient's parent or a third party requests access to the patient's PHI?

There may be instances where you are asked to disclose PHI to a patient's parents or a third party, like a lawyer or mediator, including in situations where the parents have separated or

divorced. Regardless of the parents' marital status, you must first consider whether consent must be obtained directly from the child patient. *PHIPA* presumes that individuals aged 16 and older are capable of consenting to the collection, use, or disclosure of their PHI, but the test for capacity is not strictly age-dependent: if the information relates to a treatment decision the child patient has made, you must obtain consent from the patient directly, even if they are accompanied by parent(s) or guardian(s).

If parental consent is needed, the parents' marital status will inform whether either parent may consent or if the consent of both parents is required. A family court order or the terms of a separation agreement may specify who has access to, and may make decisions about, the child's PHI. It is best practice to request a copy of the applicable court order or separation agreement prior to releasing any information, and to keep it in the patient's medical record.

Finally, *PHIPA* states that where the child patient under age 16 is capable of consenting to the collection, use or disclosure of their PHI, their decision will govern over a conflicting decision of their parent or guardian.

How do I manage a request for PHI in the context of couple, family, or group therapy?

Where therapy is being provided in a group setting, the express consent obtained from the patients will generally set out how their PHI will be shared amongst the therapy participants. However, special considerations may apply where PHI is recorded as part of an assessment of an individual patient within a group therapy context, or where a patient receives a combination of individual and group therapy. Be mindful that the patient may not have consented to sharing this specific PHI with the group and that you may need to protect it accordingly.

Where a third party (e.g. a mediator, lawyer, or the court) requests records relating to couple, family, or group therapy, the general *PHIPA* rule applies: you may not disclose PHI without patient consent unless permitted or required to so by law. In a therapy setting involving more than one patient, consent may be required from all the patients involved in the therapy, and the consent will need to be specific to the material requested.

Can I use PHI for research purposes?

Physicians sometimes undertake research using their own patients as participants. In other cases, they are requested by industry to identify eligible patients or to release general patient data for research that will be conducted by third party researchers.

PHI must only be used or disclosed for research purposes with patient consent or as permitted by law – that is, where the research ethics board that has approved the research has concluded that it is impractical to obtain patient consent and proper safeguards have been put in place.

Where PHI will be used or disclosed (either with consent or as permitted by *PHIPA*), you are reminded to only use or disclose as little PHI as possible to meet the research needs and to de-identify the PHI whenever possible or required.

For further information see the CPSO's *Physicians' Relationships with Industry: Practice, Education and Research* policy.

What are my obligations as an Independent Medical Examiner (IME)?

An IME is a physician who provides a third party report about an individual with whom the physician does not have a treating relationship. These reports are prepared for a third party process (e.g. a legal proceeding), instead of for a health care purpose, and the information collected in the course of an independent report is not considered PHI. The provisions of PHIPA therefore do not apply; instead, the federal Personal Information Protection and Electronic Documents Act will apply to the collection, use, and disclosure of personal information for this purpose. Given that different rules govern the preparation of third party reports and the conduct of a medical expert, please see the CPSO's *Third Party Reports* and *Medical Expert: Reports and Testimony* policies for further information.

e-Communication

What are the benefits and risks of e-communication?

Technology has provided physicians and patients alike with a more efficient way of maintaining and communicating PHI. The CPSO recognizes and encourages physicians to capitalize on the advantages that electronic record-keeping and e-communications have to offer.

At the same time, one of the major risks of using modern technology to communicate PHI is that the PHI will be inadvertently disclosed to someone who should not have it. This can happen in a variety of ways:

- Wifi networks and telemedicine communications can be unsecure (particularly free wifi networks in public places);
- Emails can be sent to the wrong recipient or otherwise intercepted;
- Unauthorized readers can access computer files;
- Mobile devices can be lost or stolen; and
- Erased hard drives or USBs can contain private information.

Keep these risks in mind when considering whether e-communication is appropriate in the particular circumstance.

Where can I find more information about how to interpret and apply the expectations relating to strong passwords and encryption?

The IPC provides guidance regarding the meaning of "strong passwords" and "strong encryption", including in their documents titled *Safeguarding Privacy on Mobile Devices* and *Health-Care Requirement for Strong Encryption*.

What are "reasonable security safeguards" in relation to e-communication?

Reasonable security safeguards can refer to a range technical, physical, and administrative measures, including policies, practices, and software, that collectively serve to protect PHI when it is communicated electronically between physicians (or between physicians and patients). There is no precise definition of a "reasonable security safeguard"; the kind of safeguards that will be reasonable in the circumstances will depend on a variety of factors, including the sensitivity of the PHI being communicated, the volume and frequency of the communications, and whether there is an emergency or other urgent circumstances.

The IPC provides examples of technical, physical, and administrative safeguards in its Fact Sheet: Communicating Personal Health Information by Email (September 2016).

What considerations apply when I wish to communicate electronically with patients?

As noted in the policy, you must obtain and document the patient's express consent prior to communicating electronically with patients. As a way of recording the patient's express consent, you are advised to consult the written consent form template prepared by the CMPA.

You must also use your professional judgment to determine whether this form of communication is appropriate in the particular circumstance and for the contemplated use. In making this determination, you are advised to consider:

a. the degree of sensitivity of the PHI being conveyed;
b. the frequency of communication;
c. the purpose of the communication;
d. the patient's expectations;
e. the availability of alternative methods of communication; and
f. any time-sensitive or emergency considerations.

Ultimately, e-communication may be best suited for minor tasks, such as scheduling appointments and appointment reminders, and not for urgent messages or time-sensitive health issues.