Protecting Personal Health Information

Policies of the College of Physicians and Surgeons of Ontario (the "College") set out expectations for the professional conduct of physicians practising in Ontario. Together with the *Practice Guide* and relevant legislation and case law, they will be used by the College and its Committees when considering physician practice or conduct.

Within policies, the terms 'must' and 'advised' are used to articulate the College's expectations. When 'advised' is used, it indicates that physicians can use reasonable discretion when applying this expectation to practice.

Definitions

Circle of care: the group of health care providers treating a patient who need the patient's personal health information in order to provide health care. A person outside a patient's circle of care would include:

- a person or entity who is not a health care provider (e.g. family, friends, the police, an insurance company, or the patient's employer); and
- another health care provider, including a physician, where the PHI is being provided for a purpose other than providing health care to the patient (e.g. for market research).

For further information and examples, see the *Advice to the Profession* document.

E-Communications: electronic communication tools including email, messages transmitted through electronic medical record platforms, online forums, patient portals, social media applications, instant messaging and texting, and telemedicine (including audio and videoconferencing).[1]

Lockbox: a term used to describe a patient's express instruction to withhold or withdraw their consent to share all or part of their personal health information with another health care provider.[2]

Mobile device: includes, for example, a mobile phone, laptop, USB drive, external hard drive, tablet, and wearable device.

Personal health information (PHI): any information relating to a person's health that identifies the person, including, for example, information about their physical or mental health, family

[1] See the CPSO's *Telemedicine* policy for additional expectations regarding telemedicine.
[2] When proclaimed in force, Part V.1 of the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A (hereinafter "*PHIPA*") will govern "consent directives" and "consent overrides," which are similar concepts to the lockbox in the context of the provincial Electronic Health Record.

health history, information relating to payments or eligibility for health care, and health numbers.[3]

Substitute decision-maker (SDM): a person authorized to consent on behalf of a patient to the collection, use, or disclosure of PHI about the patient.

Policy

This policy includes legislative requirements and professional obligations of physicians related to the privacy and confidentiality of patients' PHI. It does not, and is not intended to, set out all of the legislative requirements regarding privacy of PHI. Physicians are responsible for ensuring they are familiar with all of the legislative requirements; the complexity of the law in this area may warrant independent legal advice in specific circumstances.

General

1. Physicians **must** only collect, use, or disclose a patient's PHI:

    a. with the consent of the patient or SDM, and where it is necessary for a lawful purpose; or
    b. where permitted or required by law.

2. Physicians **must** collect, use, and disclose a patient's PHI only:

    a. as necessary in the course of their duties; and
    b. to the extent that it is reasonably necessary to meet the purpose for which it is being collected, used, or disclosed.

Obtaining Consent to Collect, Access, Use, or Disclose PHI[4]

Under the *Personal Health Information Protection Act, 2004*, consent may be either express or implied.[5] Physicians who have received PHI from the patient, SDM, or another health care provider for a health care purpose can rely on the patient's implied consent to disclose the PHI within the patient's circle of care, unless they have reason to believe that the patient has expressly withheld or withdrawn consent to do so.

---

[3] This list is non-exhaustive; a full legislative definition, along with certain exceptions, is found s. 4 of *PHIPA*.
[4] While *PHIPA* establishes rules about the collection, use, and disclosure of PHI, this policy largely focuses on expectations related to disclosure given the particular relevance to physicians' practice.
[5] Express consent is direct, explicit, and unequivocal, and can be given either verbally or in writing. Implied consent is inferred from the words or behaviour of the patient, or surrounding circumstances, such that a reasonable person would believe that consent has been given, although no direct, explicit, and unequivocal words of agreement have been given.

3. Except as permitted or required by law, physicians **must** obtain the patient's express consent before:

    a. collecting, accessing, or using PHI where the physician is outside the patient's circle of care in the circumstances; and
    b. disclosing PHI to a person who is outside the patient's circle of care.

4. For consent to be valid, be it express or implied, physicians **must** ensure that it:

    a. is a consent of the patient, if the patient is capable of consenting, or the SDM, if the patient is incapable;[6]
    b. is reasonable to believe that the patient knows the purposes of the collection, use, or disclosure, and that they may give or withhold consent;[7]
    c. relates to the information; and
    d. is not obtained through deception or coercion.[8]

Consent from Minors

The rules governing consent to decisions involving personal health information are found in the *Personal Health Information Protection Act, 2004* and are different from those governing consent to treatment found in the *Health Care Consent Act, 1996*.[9]

5. Physicians **must** obtain consent from the patient, regardless of the patient's age, if:

    a. the patient is capable of consenting to a decision about their PHI; or
    b. the information relates to a treatment decision[10] the patient has made.

6. Where the patient is capable of consenting to a decision about their PHI and is younger than 16 years old, and the information does *not* relate to a treatment decision[11] the patient has made, the patient's parent is also permitted by *PHIPA* to give or refuse consent to a decision

[6] Patients are capable of consenting if they are able to understand information relevant to deciding whether to consent to the collection, use, or disclosure of their PHI, and to appreciate the reasonably foreseeable consequences of giving, not giving, withholding, or withdrawing their consent.
[7] Section 18(1)(b) of *PHIPA* describes this component of valid consent as "knowledgeable".
[8] See sections 18 to 28 of *PHIPA* for further information regarding the tests for consent and capacity to make decisions regarding the collection, use, and disclosure of PHI.
[9] *Health Care Consent Act, 1996*, S.O. 1996, c. 2, Sched. A (hereinafter "*HCCA*").
[10] This includes "treatment" as defined in accordance with the *HCCA* and counselling provided under the *Child, Youth, and Family Services Act, 2017*, S.O. 2017, c. 14, Sched. 1.
[11] Ibid.

about the patient's PHI; in these cases, physicians **must** respect the patient's decision over a conflicting decision by the parent.

Withholding or Withdrawing Consent

7. Except as permitted or required by law, physicians **must** respect a patient's decision to withhold or withdraw their consent to a collection, use, or disclosure of PHI.

8. Where a patient indicates an interest in creating a lockbox, physicians **must**:

    a. discuss the potential health risks and limitations associated with lockboxes with the patient; and
    b. document this discussion and the patient's decision in the patient's medical record.

9. Where the patient has not permitted the sharing of PHI that is reasonably necessary for providing care:

    a. the disclosing physician **must** notify the recipient physician or other health care provider of the fact that there is additional relevant PHI that cannot be disclosed; and
    b. the recipient physician **must** consider whether the lockbox prevents them from safely providing the treatment.

10. Where the recipient physician declines to provide non-emergency treatment due to lockbox restrictions on accessing PHI,[12] the disclosing or recipient physician, as appropriate in the circumstance, **must**:

    a. explain the decision and reasoning to the patient; and
    b. document this encounter in the patient's medical record.

Disclosures Permitted or Required by Law (Without Consent)[13]

11. Where the disclosure of PHI is permitted by law without consent, physicians **must** use their professional judgment in considering whether and how much PHI to disclose, taking into account the specific circumstances.

[12] The *HCCA* sets out the rules for obtaining consent to treatment in an emergency. See the CPSO's *Consent to Treatment* policy for expectations relating to emergency treatment.

[13] See the *Advice to the Profession* document and the CPSO's *Mandatory and Permissive Reporting* policy for circumstances in which disclosures are permitted or required by law.

12. Where PHI is to be disclosed as permitted or required by law, physicians **must** notify the patient that the disclosure will be made and why, unless notification will:

    a. pose a genuine risk of harm to the patient, the physician, the physician's staff, other patients, or other third parties; or
    b. undermine the purpose of the disclosure.

Security of Communications

13. Physicians **must** take reasonable steps to protect PHI, including protection against theft, loss, and unauthorized access, use, and disclosure of PHI.

14. In particular, physicians **must** take reasonable steps to protect PHI from being inadvertently disclosed without authorization through:

    a. in-person and telephone conversations, including as a result of being overheard by others (e.g., staff or patients in reception or emergency room areas);
    b. voicemail messages left for patients, taking into account that more than one person may have access to voicemail at the patient's home or office;
    c. faxes, including as a result of being sent to, or intercepted by, unintended recipients; and
    d. email, telemedicine, social media, and any other form of e-communication.

15. Physicians communicating PHI electronically **must** use technology with reasonable security safeguards in place to protect the PHI, including:

    a. strong, up-to-date, industry-standard encryption;
    b. strong passwords; and
    c. secure wireless networks.

16. Physicians communicating PHI electronically with colleagues **must** be reasonably assured that the technology being used by the colleague has reasonable security safeguards in place to protect the PHI, such as those listed in provisions 15.a., b., and c.

17. Physicians wishing to communicate PHI electronically with patients **must**:

    a. obtain and document the patient's express consent to this form of communication; and

b. use their professional judgment to determine whether unsecure sharing is appropriate in the particular circumstance and for the contemplated use.

18. When obtaining the patient's express consent to the unsecure communication of PHI electronically, physicians **must** inform the patient about:

    a. how this kind of e-communication will be used;
    b. the type of information that will be communicated;
    c. how the e-communication will be processed; and
    d. the limitations and risks of using unsecure e-communication.

Security of Mobile Devices and the Cloud

19. When using mobile devices or cloud-based servers to access, store, or back up PHI – even temporarily – physicians **must** have in place reasonable security safeguards to protect PHI, including:

    a. strong, up-to-date, industry-standard encryption;
    b. strong passwords; and
    c. secure wireless networks.

Photographs and Video Recordings

20. If photographs or video recordings of a patient are required for the purpose of providing care, physicians **must**:

    a. inform the patient about the purpose of the photograph or recording;
    b. obtain express consent before taking a photograph or recording that identifies the patient; and
    c. include a copy of the photograph or recording in the patient's medical record.

Privacy Breaches

21. Physicians **must** comply with all applicable legislative and regulatory requirements in the event of a privacy breach, including notification and reporting requirements.[14]

[14] See the *Advice to the Profession* document for further information regarding privacy breaches.