Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

DELIVERED VIA EMAIL

November 10, 2017

Policy Department
College of Physicians and Surgeons of Ontario
80 College Street
Toronto, Ontario
M5G 2E2

Re: Feedback from the Information and Privacy Commissioner on the College of Physicians and Surgeons of Ontario's policy on *Medical Records*

The Information and Privacy Commissioner of Ontario (IPC) has reviewed the College of Physicians and Surgeons of Ontario's (the College) policy on *Medical Records* (the policy). The IPC has five recommendations to help the policy more clearly articulate physicians' legal and professional obligations with respect to medical records.

(1) Clarify the Language Regarding the Theft, Loss or Unauthorized Use or Disclosure of Personal Health Information

The policy's section on "Security and Storage" addresses the requirement to notify patients in cases where a physician becomes aware that personal health information over which he or she has custody or control has been "stolen, lost, or accessed by unauthorized persons". The IPC recommends that the wording of this section more closely align with the language in the *Personal Health Information Protection Act, 2004* (*PHIPA*). The policy should specify that notification to the patient is required if a physician becomes aware that personal health information over which he or she has custody or control is "**stolen or lost or if it is used or disclosed without authority**." This language would more clearly articulate physicians' obligations.

(2) Require Notification to the Commissioner

As of October 1, 2017, section 12(3) of *PHIPA* requires health information custodians to notify the Commissioner in certain circumstances when personal health information is stolen, lost or used or disclosed without authority. The IPC recommends that the policy's section on "Security and Storage" also include information regarding this requirement.

(3) Clarify Policy on Communicating Personal Health Information by Email

In the section on "Security and Storage", the policy states that "physicians who wish to send personal health information by e-mail must obtain express consent to do so from the patient or

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

their representative unless they have reasonable assurances that the information sent and received is secure." The IPC recommends that the policy more closely follow and refer to the IPC's guidance document titled "Communicating Personal Health Information by Email".

For example, the policy should clarify that physicians, as health information custodians, must implement technical, physical and administrative safeguards to protect personal health information, a requirement that applies to any email communications involving this type of information.

The policy should also require that email communication of personal health information among custodians be secured from unauthorized access by use of encryption, barring exceptional circumstances.

In regard to email communication between custodians and their patients, the policy should require custodians to use encryption where it is feasible. If encryption is not feasible, custodians should be required to determine whether it is reasonable to communicate with their patients through unencrypted email. The policy should require physicians to develop and implement a written policy for sending and receiving personal health information by email. They should have to notify their patients about this policy and obtain consent prior to the use of unencrypted email. Consent should be in plain language and indicate the types of information that may or may not be communicated by unencrypted email, the risks of using unencrypted email and the circumstances where the physician will use unencrypted email.

(4) Require Secure Transfer of Medical Records

The policy's section on "Retention, Access and Transfer of Medical Records" does not clearly state the requirement for a health information custodian to ensure that records of personal health information that are in its custody or control are transferred in a secure manner, as required by section 13(1) of *PHIPA*. The IPC recommends including this requirement in the policy.

(5) Clarify What Will Happen to Medical Records When Physician Leaves an Employment Setting or Group Practice

The policy's section on "Retention, Access and Transfer of Medical Records" is also unclear regarding what happens to medical records when a physician leaves an employment setting or a group practice.

With respect to employment, the policy states:

> Physicians who are employees must ensure that there is a written agreement with the employer about patient record retention, access and transfer. Such an agreement would be particularly useful in the event that a physician leaves practice with an employer. Where physicians are concerned that the facility's record-keeping practices may not meet the requirements of this policy, they

> are encouraged to contact the College's Physician Advisory Service for advice.

With respect to the dissolution of a group practice, the policy states an expectation that physicians have an agreement in place and addresses some of the content of that agreement. The policy further states:

> If a group practice dissolves, the patient should be asked whether he or she wishes to continue seeing a physician from the dissolved practice. If the patient is following a physician to a different practice location, the records should be transferred and physicians should agree how the cost of copying and transferring records will be divided within the group…

Unfortunately, the policy is unclear on how the above guidance relates to the requirement to "retain" medical records in section 19 of O. Reg 114/94 under the *Medicine Act, 1991,* and does not expressly address what happens when a physician leaves a group practice and the practice does not dissolve.

The IPC recommends that the policy clearly articulate, in a manner that is compliant with *PHIPA*, when physicians will, and will not, be expected to retain medical records when departing from employment or a group practice. This guidance should also expressly address both the dissolution of a group practice or employer, and where the group practice or employer continues to operate after the departure of a physician.

The policy is also unclear regarding what, specifically, should be contained in the written agreement between the departing physician and the employer. The IPC further recommends that the policy clearly articulate, in a manner that is compliant with *PHIPA,* what must be contained in the agreement between the physician and the employer.

In revising the policy to clarify the above points, it is the IPC's view that a valid patient consent under *PHIPA* should be the primary consideration in deciding if medical records will be provided to a physician departing from a group practice or employer. This consent should be provided to, and considered by, the health information custodian of the record under *PHIPA.* In the absence of consent, *PHIPA* generally does not permit health information custodians to disclose personal health information to an agent who is departing the practice and will no longer be providing health care to the individual. Of course, if the departing physician is the health information custodian of the medical records, then such consent would not be required.

Thank you for considering our recommendations.