September 9, 2014

Via Mail and Email: PIPACommittee@leg.bc.ca

Special Committee to Review the *Personal Information Protection Act*
Parliamentary Committees Office
Room 224, Parliament Buildings
Victoria, British Columbia V8V 1X4

Dear Committee Members:

Re: Review of *Personal Information Protection Act*

The Canadian Medical Protective Association ("CMPA") welcomes the opportunity to participate in the review of the *Personal Information Protection Act*.

As you may be aware, the CMPA is a not-for-profit mutual defence organization operated for physicians by physicians. It is the principal provider of medical-legal assistance to Canadian physicians, including physicians in British Columbia. In addition to providing legal representation to its members, the CMPA provides broader advisory services on a multitude of medical-legal issues including risk management, quality assurance, research and education. Informing physicians about their legal and ethical obligations is an important element of the CMPA's advisory services to its members.

Health-Specific Privacy Legislation

1. *General Comments*

As the Committee is likely aware, most Canadian jurisdictions have now enacted health-specific privacy legislation that is broadly applicable to the collection of personal health information by healthcare providers. In the CMPA's view, there would be significant value in British Columbia developing health-specific privacy legislation, which would provide a framework for the collection, use, and disclosure of personal health information in a healthcare setting. There are unique issues that arise in the healthcare environment that are best addressed by specific legislation. We understand that the Information and Privacy Commissioner for British Columbia ("IPC") has recommended the creation of health-specific privacy legislation for the province and we fully support this recommendation.

Currently, *PIPA* governs the management of personal information by physicians in their private practice, whereas the *Freedom of Information and Protection of Privacy Act* ("*FOIPPA*") ensures the privacy of personal information held by public bodies, *e.g.* hospitals. This overlap of legislation is unnecessarily complex and can lead to confusion amongst healthcare professionals

about which legislation applies in the circumstances. For example, physicians often work in various practice settings. In this regard, physicians may maintain their own private offices and as well hold privileges at a hospital. It is also not unusual for the same patient to seek treatment from a physician in his/her private office and later that day attend at the hospital for specific laboratory testing or imaging. In these circumstances, it can be challenging to determine which privacy legislation applies. It is therefore preferable to have one privacy statute that applies to all personal health information, regardless of the type of healthcare setting in which the information is accessed, collected, used and disclosed.

2. Governance Framework for Electronic Health Records

A further impetus for developing health-specific privacy legislation is the proliferation of electronic health records (EHR). The *E-Health Act* governs information stored in designated health information banks, but it does not address the management of personal health information contained in the (eventual) province-wide EHR. The CMPA understands the Ministry of Health is of the view that the province-wide EHR is the "cornerstone of the Province's eHealth strategy to deliver faster and more effective treatment to patients."[1] Health-specific privacy legislation would provide an appropriate framework for overseeing the management of information contained in the province wide EHR. As the province-wide EHR expands, the desire to use data analytics for health system planning will increase. Health-specific privacy legislation that provides an effective governance framework will ensure a balance could be achieved between protecting the privacy of personal health information and subsequent use of that information through data analytics.

In the context of interoperable EHRs, it is extremely important that all key stakeholders participate in the governance process and understand each other's respective obligations so that these varying obligations can be anticipated in advance and incorporated into an effective governance framework. Issues such as consent for the transfer of personal health information into an EHR and the limited purposes for which patient information can be used and shared without consent, are fundamental aspects of an EHR governance framework that must be fully debated by interested stakeholders.

The CMPA has worked with stakeholders in other jurisdictions with respect to various EHR issues and would also be pleased to provide any assistance in this regard. The CMPA is aware that other jurisdictions, including Alberta, have adopted a similar governance structure for the development of EHRs and doing so has, to date, functioned very well to ensure the interests of all affected parties (*e.g.* patients, healthcare providers, regulators, etc.) are respected in the EHR environment.

[1] Ministry of Health, http://www.health.gov.bc.ca/ehealth/ehr.html (accessed on August 15, 2014)

Personal Information Protection Act

In the event that health-specific privacy legislation is not introduced in British Columbia, the CMPA is pleased to provide suggestions for improvement of *PIPA.* In particular, the CMPA submits amendments to *PIPA* are required to expressly recognize the important role the CMPA and other similar organizations perform for patients and physicians with respect to medical-legal advice, error reduction and risk management activities.

1. Risk Management Advice

It is imperative that *PIPA* not hinder health care providers' ability to communicate patients' personal health information to their medico-legal protection providers (including the CMPA). Error and risk management efforts that contribute to a recognized higher quality of care could be seriously curtailed in circumstances where physicians and other health care providers feel that they are not free to seek necessary advice or guidance as the result of privacy legislation.

The Special Committee will be interested to know that many jurisdictions that have enacted health-specific privacy legislation specifically authorize the disclosure of health information without consent where the disclosure is required for the purpose of obtaining error or risk management services.[2]

The CMPA submits that it would therefore be appropriate for *PIPA* to be amended to expressly permit the disclosure of personal information without consent if the disclosure is required for the purpose of obtaining error or risk management services.

This issue could be addressed by incorporating specific reference to error and risk management services into subsection 18(1), as follows:

> 18 (1) An organization may only disclose personal information about an individual without the consent of the individual, if
> …
> (q) the disclosure is to the organization's insurer or professional liability provider for the purpose of obtaining error or risk management services.

[2] Manitoba's *Personal Health Information Act*, s. 22(2)(e)(iv); Ontario's *Personal Health Information Protection Act*, s. 37(1)(d); New Brunswick's *Personal Health Information Privacy and Access Act*, s. 34(1)(f) and 38(1)(g); Nova Scotia's *Personal Health Information Act*, s. 35(1)(j) and s. 38(1)(t); Newfoundland and Labrador's *Personal Health Information Act*, s. 34(d) and s. 39(1)(d); Prince Edward Island's *Health Information Act*, s. 22(1)(f) and 23(130(g); Northwest Territories' *Health Information Act*, s. 35(d)(vi) and s. 53(b); and Yukon's *Health Information Privacy and Management Act*, s. 56(1)(m) and s. 58(k).

2. Contemplated or Actual Proceedings

All jurisdictions that have enacted privacy legislation recognize that the disclosure of personal information without consent is permissible for the purpose of a proceeding. Although *PIPA* does allow for such a disclosure under subparagraph 18(1)(c), the CMPA respectfully submits that amending this exception could better facilitate the disclosure of personal information where it is required for a proceeding.

As it is currently worded, disclosure without the consent of the individual is only permitted where "it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is reasonable for purposes related to an investigation or a proceeding."

The disclosure of personal information for the purpose of reasonably contemplated proceedings in which the organization is likely to be a party is also generally considered to be a valid disclosure of personal information (*e.g.* see Manitoba's PHIA (subparagraph 22(2)(k)) and Ontario's *PHIPA* (subparagraph 41(1)(a)). It may very well be that subparagraph 18(1)(c) is intended to include those proceedings that while anticipated, have not yet been commenced. Disclosures to legal counsel in these circumstances would also clearly be permitted under the common law doctrine of solicitor-client privilege. However, for the sake of greater clarity, the CMPA submits that the definition of "proceedings" be slightly amended to specifically include anticipated proceedings.

In order to ensure that physicians and other health care providers are not unnecessarily restricted in the disclosure of personal information for the purpose of proceedings that are either contemplated or have been commenced, the CMPA suggests the following amendments to subparagraph 18(1)(c) and to the definition of "proceeding" found in section 1:

> "proceeding" includes anticipated proceedings and means a civil, criminal or administrative proceeding that is related to the allegation of:
> ...
>
> 18 (1) An organization may only disclose personal information about an individual without the consent of the individual, if
> …
>
> (c) the disclosure is reasonable for purposes related to an investigation or a proceeding.

Similarly, it is important that organizations be permitted to use personal information in these circumstances. Consequently, subparagraph 15(1)(c) should also be amended as follows:

> 15(1) An organization may use personal information about an individual without the consent of the individual, if
> …
>
> (c) the use is reasonable for purposes related to an investigation or a proceeding.

3. Mandatory Breach Notification

The CMPA is aware that the IPC has indicated to the Special Committee that her office's main recommendation for reforming *PIPA* is to incorporate a mandatory duty to notify the Commissioner and affected individuals in the event of a privacy breach that creates a real risk of significant harm. [3]

To the extent the Special Committee agrees with the IPC's recommendation, it would be preferable that any breach notification provision recognized that there may be circumstances in which notification is not required, such as where the breach is unlikely to result in harm to the affected individual or where notification may actually give rise to a risk of harm to an individual.

For example, if a lost or stolen electronic storage device (*e.g.* computer hard drive) containing personal information was properly encrypted, it is generally considered not to be necessary to notify the individual since the information cannot be accessed without an encryption key. Similarly, in some cases, disclosure of the breach may cause harm (*e.g.* psychological harm) to the individual that would militate against disclosure.

The Special Committee may be aware that privacy legislation in a number of other jurisdictions in Canada contemplates that notification may not be required in all cases of a privacy breach and is dependent upon the likelihood of harm arising from the loss or theft of personal information. For example, subsections 15(3) through (7) of Newfoundland and Labrador's *Personal Health Information Act* state that notification of the individual about a privacy breach may not be required where there is a reasonable belief that the breach will not have an adverse impact on the individual, or unless the Privacy Commissioner directs otherwise. The CMPA encourages a similar threshold risk assessment for any breach notification requirement within *PIPA*.

Conclusion

[3] General Briefing for the Special Committee to Review the *Personal Information Protection Act* (May 28, 2014).

The CMPA is grateful for the opportunity to make submissions regarding the review of *PIPA*. We are hopeful that the Special Committee will consider our comments when drafting its recommendation in the Final Report. The CMPA would be pleased to engage in further discussions regarding any of the comments set out above.

Yours sincerely,

Hartley S. Stern, MD, FRCSC, FACS
Executive Director/Chief Executive Officer

HSS/lg

C: Dr Edward Crosby, President
Dr Paul Farnan, Councillor
Dr Barbara Kane, Councillor
Dr David Naysmith, Councillor

Bc: Mr Domenic A. Crolla
Ms Barbara Norell (Harper Grey)
Corporate Management Committee