JUNE 2020

Comments of the Information and Privacy Commissioner of Ontario on Proposed Regulations Under Part V.I of *PHIPA*

Brian Beamish
Commissioner

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

INTRODUCTION

The May 2, 2020 edition of the Ontario Gazette contains a notice by the Minister of Health of proposed regulations (the Proposed Regulations) under the *Personal Health Information Protection Act, 2004* (*PHIPA*).

The Proposed Regulations are another step towards bringing Part V.1 of *PHIPA* into effect. Part V.1 of *PHIPA* was passed in 2016 as part of Bill 119*, Health Information Protection Act, 2016* and contains the framework for regulating the provincial electronic health record (the EHR). While the Information and Privacy Commissioner of Ontario (IPC) supports most of the Proposed Regulations, certain provisions, if passed, will be a step backward on the path to the development and implementation of a robust and privacy protective EHR framework in Ontario.

The shortcoming in the Proposed Regulations relates to consent granularity. Under Part V.1, individuals have the right to control how their health information will be shared for health care purposes through "consent directives." For example, consider an individual who does not want their ex-spouse who works for a health information custodian (e.g. a hospital) to access their health information. In that case, the individual would want to implement a consent directive to block a particular agent (their ex-spouse) from accessing their information in the EHR, while continuing to allow their treating health care providers to have access. As the example illustrates, for individuals to effectively exercise their rights under Ontario's health privacy law, the technology behind the EHR must be granular enough to allow different types of information to be blocked for different agents and custodians. However, the Proposed Regulations only contain one option. They only allow an individual to block everything from everyone or block nothing. In the absence of less restrictive options, this is not a meaningful choice.

As explained in more detail below, Ontarians will have fewer rights to control their health information after this regulation comes into force than before. The government will not even promise to keep the current consent granularity options available for individuals wishing to exercise their rights in the future. Ontario's electronic health information infrastructure is moving in the wrong direction.

Back in 2012, the Ontario government committed to the IPC that it would implement regulations to provide individuals with five specific consent granularity options (explained below). Over the course of many years, representatives of the Ministry of Health and eHealth Ontario (now Ontario Health) continued to refer to these five consent granularity options and to indicate that they would be available in the EHR. Despite this, the work necessary to give effect to these five consent granularity options and to ensure Ontarians can meaningfully control access to their personal health information was never completed.

The submission that follows explains the IPC's concerns about consent granularity in more detail and provides additional comments on the Proposed Regulations.

1. CONSENT GRANULARITY

A. ENSURE INDIVIDUALS HAVE BROAD CONSENT OPTIONS

As mentioned in the introduction, *PHIPA* gives individuals the right to decide when and how their personal health information will be shared for health care purposes. In the context of the EHR, this right is operationalized through consent directives.

The IPC wants to ensure that individuals have meaningful options to exercise their right to control access to their health information and to ensure that the consent directives, which implement this right, correspond to the common privacy concerns encountered by the IPC. To that end, in 2012, the IPC and the government discussed this issue and the government agreed to implement regulations to provide individuals with five options for issuing consent directives in the EHR. These options are:

- **Agent:** this directive prevents a specific agent (e.g. employee, staff member or volunteer) of a custodian from viewing an individual's health information,
- **Domain:** this directive prevents anyone from viewing an individual's health information in a clinical domain repository such as the Ontario Laboratories Information System,
- **Health information custodian-agents:** this directive prevents anyone at a specific custodian from viewing an individual's health information,
- **Health information custodian-records:** this directive prevents anyone from viewing an individual's health information contributed to the EHR by a specific custodian, and
- **Global consent directives:** this directive prevents anyone from viewing any part of an individual's health information in the entire EHR.

These five consent granularity options give individuals a broad range of choices to implement their rights, while still ensuring the effective provision of health care.

With the Proposed Regulations, the government is only providing individuals with one option to control access to their health information – global consent directives. Subsection 18.4 (3) of the Proposed Regulations states:

> Where an individual makes a consent directive, **it applies to all** of the individual's personal health information that is accessible by means of the electronic health record, **unless it is reasonably possible** for the prescribed organization [Ontario Health] to apply the consent directive only to the specific personal health information that has been identified by the individual, in which case the consent directive applies only to that personal health information [emphasis added].

While the Proposed Regulations refer to the possibility of more granular consent directives where "reasonably possible," the IPC is sceptical given the government's failure to proceed with the five consent granularity options it had previously committed to and given that the government has not committed to giving individuals who wish to make consent directives in the EHR the same rights that exist now. This means that individuals who have already made a consent directive in systems that will become the EHR have more rights than individuals who will make a consent directive in the EHR in the future. The government's intentions appear to be clearly set out in the summary of the Proposed Regulations in the Gazette, which states that the Proposed Regulations "[p]rescribe the level of specificity ('granularity') at which personal health information may be subject to a consent directive" and that **"[t]he granularity is set at the entirety of the electronic health record** [emphasis added]."

This 'all or nothing' choice is not a true choice in the absence of less restrictive options, and may cause some individuals not to protect their health information out of fear that implementing a consent directive will affect their health care by limiting the availability of their health information to their health care providers. The government may argue this fear is unfounded because consent directives can be overridden in certain circumstances, including with the consent of the individual. However, this is not a good solution. Consent overrides are administratively demanding. When a consent directive is overridden, the health information custodian must notify the individual and, in certain circumstances, the IPC. Further, the organization that is responsible for developing and monitoring the EHR (Ontario Health) must audit, monitor, and log consent overrides and notify custodians of overrides. This is necessary to ensure that health information subject to consent directives is not being viewed for unauthorized purposes.

The Proposed Regulations will likely cause more consent overrides and, ultimately more administrative work for already burdened health care providers as well as Ontario Health. The Proposed Regulations will also likely cause the individual who issued the consent directive to be frequently asked for express consent for a consent override, placing an additional burden on patients.

More broadly, the absence of meaningful consent granularity options could undermine the entire purpose of the EHR, and force health care providers to use other information

systems where individuals can block less information because they are able to place restrictions that are more granular. Simply put, other systems will give health care providers and patients the information and choices they want.

The solution to this problem was simple. The government and eHealth Ontario (now Ontario Health) should have used the eight years since the government first committed to providing Ontarians with the five consent granularity options to build the electronic systems in the EHR in the way the government had agreed and that would allow individuals to more effectively exercise their rights to control their health information. However, that was not done. The government must give Ontarians true choices in order to effectively implement their rights and protect the privacy of their personal health information.

B. KEEP CURRENT CONSENT OPTIONS

While not a solution to the problem mentioned above, there is one small thing the government must do to protect the privacy rights that individuals currently possess. It must continue to offer the consent granularity options that are presently available. There are electronic systems that will form part of the EHR that currently offer more consent granularity options than will be offered in the broader EHR. Section 18.5 (the transitional provision) states:

> (1) Where, before section 55.6 of the Act came into force, an individual made a directive withholding or withdrawing, in whole or in part, the individual's consent to the collection, use or disclosure of personal health information that is accessible by means of the electronic health record developed and maintained by the prescribed organization, the prescribed organization shall continue to implement the individual's directive as it existed before the coming into force, subject to subsection (2).
>
> (2) Where an individual has made a directive described in subsection (1) and has subsequently made a consent directive under subsection 55.6 (1) of the Act, the prescribed organization shall implement the consent directive.

Subsection 18.5 (1) suggests that, after Part V.1 of *PHIPA* comes into effect, prior consent directives will continue to be applied with the granularity they are now. However, subsection 18.5 (2) suggests that new consent directives will not be able to be applied with the same granularity as previous directives.[1] Indeed, this is what the government has advised the IPC.

1 The IPC also notes that the drafting of section 18.5 appears to create a bizarre incentive for individuals to never change their historical consent directives for fear that they will never be able to make another directive with the same granularity.

Not only should prior consent directives continue to be implemented as they are now, but individuals should also have the right to implement new consent directives with the same granularity as they do now.[2]

2. RESPONSIBILITIES OF CORONERS AND THE PRESCRIBED ORGANIZATION UNDER SUBSECTION 55.9.1 (1) OF *PHIPA*

Part V.1 of *PHIPA* did not originally permit coroners and medical officers of health to access the EHR to carry out their statutory roles. To grant such access, Bill 188, *Economic and Fiscal Update Act, 2020* added section 55.9.1 to *PHIPA*.

In the context of coroners, access to the EHR creates a regulatory problem, namely, coroners conducting death investigations under the *Coroners Act* were likely not subject to the obligations imposed by *PHIPA*. To address this regulatory gap, section 55.9.1 of *PHIPA* allows access where prescribed requirements, if any, are met. The Proposed Regulations set out these prescribed requirements. The IPC is supportive of the requirements regulating coroners' access to the EHR, subject to the comments below.

A. ADD INDIVIDUAL NOTIFICATION REQUIREMENT TO SUBSECTION 18.10 (1)

Subsection 18.10 (1) of the Proposed Regulations sets out the provisions of *PHIPA* that a coroner must comply with when accessing personal health information in the EHR. These provisions apply to a coroner as if the coroner were a custodian under *PHIPA*.

The Proposed Regulations provide that subsections 12 (1) and 12 (3) of *PHIPA* apply to coroners, but not subsection 12 (2) of *PHIPA*. This omission is significant.

Subsection 12 (1) would require a coroner to take reasonable steps to protect health information collected from the EHR from theft, loss and unauthorized use and disclosure. Section 12 (3) of *PHIPA* would require a coroner to notify the IPC if a theft, loss or unauthorized use or disclosure of that information meets prescribed requirements. However, subsection 12 (2), which is omitted from the Proposed Regulations, would require the coroner to notify the individual of all thefts, losses and unauthorized uses and disclosures of their information.[3]

---

2 If the current consent granularity options are kept in these systems, individuals wishing to make consent directives will also have to be informed that their more granular consent directive will not be effective in other systems in the broader EHR.

3 The IPC notes that subsection 18.10 (4) requires that notice be given to the individual of an unauthorized collection. However, that provision would not apply to a subsequent unauthorized use or disclosure or a theft or loss of the information. Note that amendments to subsection 18.10 (4) are also recommended below.

The IPC recommends that coroners be required to comply with subsection 12 (2) of *PHIPA* as if they were custodians. Subsection 18.10 (1) of *PHIPA* should be amended as follows:

> **18.10** (1) A coroner to whom the prescribed organization provides information under subsection 55.9.1 (1) of the Act shall comply with section 11.1, subsections 12 (1), (2) and (3), subsection 13 (1) and sections 17, 17.1, 30 and 31 of the Act as if the coroner were a health information custodian.

B. ADDRESS THE RESPONSIBILITIES OF THE PRESCRIBED ORGANIZATION (ONTARIO HEALTH)

As noted above, section 18.10 of the Proposed Regulations sets out the responsibilities of coroners when accessing health information in the EHR. However, to ensure the responsibilities on coroners are being fulfilled, their access to the EHR must be audited, logged and monitored by Ontario Health in the same manner as for custodians. Otherwise, there is a risk that coroners' contraventions will go undetected.

Further, the Proposed Regulations should clarify that the prescribed organization, namely Ontario Health, has to comply with the practices and procedures approved by the IPC when providing coroners with access to health information from the EHR. Again, this will put coroners on equal footing with custodians accessing the EHR and prevent a legislative gap.

For the above reasons, the IPC recommends adding the following section to the Proposed Regulations.

> **Logging, auditing and monitoring access by coroners**
>
> **18.11** For greater clarity, the prescribed organization shall comply with section 55.3 of the Act in respect of personal health information provided to a coroner under subsection 55.9.1 (1) of the Act as if the coroner were a health information custodian, and shall further comply with the practices and procedures approved by the Commissioner under paragraph 14 of section 55.3 of the Act and under section 55.12 of the Act in respect of such information.

C. NARROW THE CIRCUMSTANCES IN WHICH NOTIFICATION TO THE IPC IS REQUIRED UNDER SUBSECTION 18.10 (4)

If a coroner collects health information without authority by means of the EHR, subsection 18.10 (4) requires the coroner to notify the IPC. The IPC recommends amending clause 18.10 (4) (b) to ensure that notification to the IPC is required in only

those circumstances where a custodian would be required to notify the IPC. This will put coroners on equal footing with custodians collecting health information from the EHR and ensure that the IPC is only notified of breaches that meet certain criteria, in order to ensure that resources are focused on the most significant breaches. Clause 18.10 (4) (b) should also be amended to ensure that notice to the IPC is given at the first reasonable opportunity. In particular, it is recommended that clause 18.10 (4) (b) of the Proposed Regulations be amended as follows:

> (b) notify the Commissioner of the unauthorized collection at the first reasonable opportunity under any circumstance where the coroner would be required to notify the Commissioner if the coroner were a custodian to which subsection 18.3 (1) of this Regulation applied.

3. CORRECTION OF DRAFTING ISSUES

The IPC has also noted other drafting issues with the Proposed Regulations. For ease of reference, these additional drafting issues and the IPC's recommended amendments (as well as the amendments previously mentioned in Part 2 of this submission) are set out in Appendix A. Changes are underlined and explanations are added in square brackets.

APPENDIX A: SECTIONS OF PROPOSED REGULATIONS WITH IPC RECOMMENDED AMENDMENTS

Notice requirements, clause 55.7 (7) (a) of the Act

18.7 (1) Where a health information custodian is required to notify an individual under clause 55.7 (7) (a) of the Act, the notice must include,

(a) the name of the individual to whom the information relates;

(b) the identity of any health information custodian that disclosed the information;

(c) a general description of the information, other than personal health information, that was collected;

(d) the date and time of the collection;

(e) the reason or reasons for the consent override as described in subsection 55.7 (1), (2) or (3) of the Act and the reason or reasons the personal health information was necessary for each purpose;

[IPC change recommended to be consistent with clause 18.8 (1) (c) of the Proposed Regulations]

(f) the name of the individual, including a substitute decision-maker, who provided express consent under subsection 55.7 (1) of the Act, if applicable;

(g) the name of any agent of the health information custodian who authorized the override;

(h) contact information for the health information custodian that collected the information; and

~~(i) contact information for and information about the process of filing a complaint with the Commissioner; and~~

(~~j~~ i) contact information for the Commissioner and the fact that the individual may make a complaint to the Commissioner under Part VI of the Act.

[IPC changes recommended because clause 18.7 (1) (i) in the Proposed Regulations created the same obligation as clause 18.7 (1) (j)]

…

Provision to coroner

18.10 (1) A coroner to whom the prescribed organization provides information under subsection 55.9.1 (1) of the Act shall comply with section 11.1, subsections 12 (1), (2) and (3), subsection 13 (1) and sections 17, 17.1, 30 and 31 of the Act as if the coroner were a health information custodian.

[IPC change recommended under Part 2 of this submission]

(2) Despite any other provision in the Act or the regulations, a ~~A~~ coroner to whom the prescribed organization provides information under subsection 55.9.1 (1) of the Act may only use or disclose the information for the purpose for which the information was collected or as required by law.

[IPC changes recommended to be consistent with section 31 and subsection 55.5 (5) of *PHIPA*]

…

(4) If personal health information about an individual is collected without authority by a coroner by means of the electronic health record, the coroner shall,

(a) notify the individual at the first reasonable opportunity of the unauthorized collection and include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI of the Act; and

(b) notify the Commissioner of the unauthorized collection at the first reasonable opportunity under any circumstance where the coroner would be required to notify the Commissioner if the coroner were a custodian to which subsection 18.3 (1) of this Regulation applied.

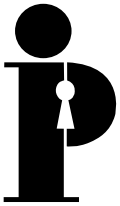
[IPC change recommended under Part 2 of this submission]

…

Logging, auditing and monitoring access by coroners

18.11 For greater clarity, the prescribed organization shall comply with section 55.3 of the Act in respect of personal health information provided to a coroner under subsection 55.9.1 (1) of the Act as if the coroner were a health information custodian, and shall further comply with the practices and procedures approved by the Commissioner under paragraph 14 of section 55.3 of the Act and under section 55.12 of the Act in respect of such information.

[IPC change recommended under Part 2 of this submission]



Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: 416-326-3333

www.ipc.on.ca
info@ipc.on.ca

June 2020