AUGUST 2020

Submission of the Information and Privacy Commissioner of Ontario to the Special Committee to Review the *Personal Information Protection Act* (British Columbia)

Patricia Kosseim
Commissioner

Information and Privacy
Commissioner of Ontario

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

INTRODUCTION

The Special Committee to Review the *Personal Information Protection Act* (*PIPA*) of British Columbia has invited the public to provide input on how the Act is working.[1] The Office of the Information and Privacy Commissioner for British Columbia, in its June 2020 general briefing for the Special Committee, identified the need for mandatory breach reporting and for the ability to levy administrative monetary penalties as two of its most pressing concerns.[2] The Information and Privacy Commissioner of Ontario (IPC) makes this submission in order to provide the Special Committee with information about the mandatory breach reporting and administrative penalty provisions found in Ontario's *Personal Health Information Protection Act, 2004* (*PHIPA*) and its regulation (O. Reg. 329/04). As the Special Committee considers possible amendments to *PIPA* and the possible creation of a stand-alone health information privacy law for British Columbia, the IPC offers this information on *PHIPA* as a comparable model that the Special Committee may wish to consider.

In recent years, Ontario has made a number of amendments to *PHIPA* to account for the fact that personal health information is collected, used and disclosed in an increasingly digital format, and that various health care providers must increasingly share individuals' personal health information with one another in order to deliver care in a coordinated, effective manner.

For example, recent amendments to *PHIPA* were designed to facilitate the sharing of personal health information among members of Ontario Health Teams (a new way of organizing and delivering care in the province) by expanding the definition of "health information custodian" to include a "person or entity that is part of an Ontario Health Team and that provides a home and community care service …" Another amendment (and a forthcoming regulation that will correspond to it) will set out the ways in which health information custodians can provide personal health information to "consumer electronic services providers" (e.g. health-related apps used by individuals) in order to enable more innovative means of obtaining health services. Yet a further amendment will allow Ontario Health to provide personal health information to a coroner in relation to an investigation conducted under Ontario's *Coroners Act*.

However, enabling greater sharing of personal health information among more actors in the health system also exposes that information to greater risks, such as cyber security risks or unauthorized access. The Ontario Premier's Council on Improving Healthcare and Ending Hallway Medicine recommended that "[m]odernized legislation should

1 Special Committee to Review the *Personal Information Protection Act*, **https://www.leg.bc.ca/parliamentary-business/committees/41stParliament-5thSession-pipa**.

2 Information and Privacy Commissioner for British Columbia, "General Briefing for the Special Committee to Review the Personal Information Protection Act" (June 2020), pp. 10-11, **https://www.oipc.bc.ca/special-reports/2426**.

find the right balance between improving comprehensive access to personal health information and keeping the information secure."[3]

The IPC agrees that strong oversight and security safeguards to protect individuals' personal health information are integral components of a modern and effective health information protection regime. Given the fundamental changes to the way health care is delivered in Ontario, the IPC has remarked that "it is of utmost importance that appropriate frameworks and safeguards be put in place to protect the privacy and access rights of Ontarians and to ensure accountability and transparency within the health system."[4]

Recognizing the need to counterbalance the added security risks associated with increasing access to personal health information, the Ontario government strengthened the mandatory breach reporting regime under *PHIPA* in 2017 to include an explicit reporting mechanism to the IPC. More recently, the Ontario government passed Bill 188, *Economic and Fiscal Update Act, 2020* which amended *PHIPA* to include the doubling of fines for offences and the creation of an administrative penalty scheme to encourage compliance on the one hand, and dissuade illicit behaviour on the other.[5]

These administrative penalties and the strengthened mandatory breach reporting scheme are two components of *PHIPA* that help ensure the accountability of health information custodians with respect to the personal health information in their custody or under their control. Part A of this submission describes the various forms of breach reporting mandated by *PHIPA*, and Part B discusses the details of the new administrative penalty scheme.

A. MANDATORY BREACH REPORTING

1. REPORTING TO THE INDIVIDUAL

Since its enactment in 2004, *PHIPA* has contained a requirement for a health information custodian to notify an individual in the event of a breach of that individual's personal health information. The 2004 version of this provision read:

> "… a health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable

3 "A Healthy Ontario: Building a Sustainable Health Care System – 2nd Report from the Premier's Council on Improving Healthcare and Ending Hallway Medicine" (June 2019), p. 20, **https://files.ontario.ca/moh-healthy-ontario-building-sustainable-health-care-en-2019-06-25.pdf**.

4 Comments of the Information and Privacy Commissioner of Ontario on Bill 74 (March 29, 2019), p. 1, **https://www.ipc.on.ca/wp-content/uploads/2019/04/2019-03-bill-74.pdf**.

5 Bill 188, *Economic and Fiscal Update Act*, 2020, Sched. 6.

> opportunity if the information is stolen, lost, or accessed by unauthorized persons."[6]

Since 2004, the provision was reworded and expanded upon, so that it currently reads:

> "… if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,
>
> (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
>
> (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI."[7]

The individual notice requirement acknowledges the fact that individuals have an interest in the confidentiality of their personal health information that is in the custody or control of a health information custodian and their privacy with respect to that information. They have the right to know when that confidentiality or privacy might have been compromised; they play an active role in helping contain the breach and mitigating its adverse impacts; and they have the right to make a complaint to the IPC.

2. REPORTING TO THE IPC

There are two mechanisms by which health information custodians are required to report breaches to the IPC. First, if the circumstances surrounding a breach meet the requirements prescribed in the regulation to *PHIPA*, custodians must report details of that specific breach to the IPC when the breach occurs. Second, custodians must provide the IPC with an annual statistical report of all breaches that have occurred in the past year. Each of these two reporting mechanisms is described in turn below.

A. NOTICE TO THE IPC UNDER SUBSECTION 12 (3) OF *PHIPA*

Effective October 1, 2017, health information custodians are required to notify the IPC of only *significant* instances of theft, loss, or unauthorized use or disclosure of personal health information.[8] Therefore not every incident that requires notice to the individual will necessarily require notice to the IPC. The regulation under *PHIPA* sets out, in section 6.3, the seven circumstances in which notice to the IPC is required. This notice is required if:

---

6 *PHIPA*, subsection 12 (2) [historical version of November 1, 2004].

7 *PHIPA*, subsection 12 (2).

8 *PHIPA*, subsection 12 (3) and O. Reg. 329/04, section 6.3.

1. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority.

2. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was stolen.

3. The health information custodian has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in the custodian's custody or control, the personal health information was or will be further used or disclosed without authority.

4. The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information in the custody or control of the health information custodian.

5. The health information custodian is required to give notice to a College[9] of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.

6. The health information custodian would be required to give notice to a College, if an agent of the health information custodian were a member of the College, of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.

7 The health information custodian determines that the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances, including the following:

   i. Whether the personal health information that was lost or used or disclosed without authority is sensitive.

   ii. Whether the loss or unauthorized use or disclosure involved a large volume of personal health information.

   iii. Whether the loss or unauthorized use or disclosure involved many individuals' personal health information.

   iv. Whether more than one health information custodian or agent was responsible for the loss or unauthorized use or disclosure of the personal health information.[10]

9 In this section, "College" means a College as defined in subsection 17.1 (1) of *PHIPA*.

10 O. Reg. 329/04, subsection 6.3 (1).

The IPC has posted on its website a document titled "Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector," which interprets section 6.3 and provides instructions on how to notify the IPC.[11]

The above regulation went into effect on October 1, 2017. From October to December 2017, the number of reported breaches more than doubled to 125, when compared with 58 during the same time period in 2016.[12] In terms of the full calendar year of 2017, the number of self-reported breaches amounted to 322, and rose to 506 in 2018[13] and 564 in 2019.[14]

B. ANNUAL REPORT TO THE IPC

In addition to the requirement to report these significant breaches at the time they occur, there is a separate requirement to provide the IPC with an annual report on the total number of all breaches that have occurred in the previous calendar year. Section 6.4 of the regulation under *PHIPA* states that by March 1 of each year, a health information custodian shall provide the IPC with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.[15]

The health information custodian must count all thefts, losses, and unauthorized uses and disclosures, even if the custodian was not required to report them under section 6.3 of the regulation.

The IPC has posted on its website a document titled "Annual Reporting of Privacy Breach Statistics to the Commissioner: Requirements for the Health Sector," which explains section 6.4 and provides instructions on how to prepare the annual report.[16] For each of the four categories (theft, loss, use with authority, and disclosure without

11 **https://www.ipc.on.ca/wp-content/uploads/2017/08/2019-health-privacy-breach-notification-guidelines.pdf**.

12 2017 Annual Report of the IPC, p. 33, **https://www.ipc.on.ca/wp-content/uploads/2018/06/ar-2017-e-web.pdf**.

13 2018 Annual Report of the IPC, p. 24, **https://www.ipc.on.ca/wp-content/uploads/2019/06/ar-2018-e.pdf**.

14 2019 Statistical Report of the IPC, p. 71, **https://www.ipc.on.ca/wp-content/uploads/2020/03/ar-2019-stats-e.pdf**.

15 O. Reg. 329/04, subsection 6.4 (1).

16 **https://www.ipc.on.ca/wp-content/uploads/2017/11/annual-breach-statistics-rptg-2.pdf**.

authority), custodians are required to sort the breaches further into sub-categories set out by the IPC. For example, under the "theft" category, custodians must track whether the theft was by an internal party, was by a stranger, was the result of a ransomware attack, and so forth.

The first annual report was due on March 1, 2019, which means that the first calendar year for which custodians were required to track these statistics was 2018. For the 2018 calendar year, over 800 custodians submitted annual reports to the IPC. Collectively, these reports indicated that there were 11,278 incidences of personal health information breaches in 2018.[17] For 2019, the submitted annual reports indicated that there were 12,282 incidences of personal health information breaches.[18] Full statistics in spreadsheet format are available for download on the IPC's website.[19]

Breach reporting gives the IPC a high-level overview of the volume and types of breaches that are occurring across the health sector in Ontario and, when necessary, enables the IPC to take steps to minimize systemic issues that regularly lead to breaches. Such steps might include issuing guidance, lobbying for amendments to *PHIPA* and its regulation, and consulting with the government and providers as appropriate.

For example, the IPC had long been aware that there were many breaches relating to the transmission of personal health information by fax, but the annual statistical reports from custodians highlighted how serious the problem is. This prompted the IPC, in its 2018 Annual Report, to remark that over 6,000 of 11,278 health information privacy breaches reported for that year were due to misdirected faxes, and to call for Ontario to implement a strategy to eliminate or reduce dependence on fax machines in the health care context.[20]

Similarly, even before the self-reporting requirements were added to *PHIPA*, the IPC had identified "snooping" (i.e., unauthorized access by health professionals) as a significant category of health information privacy breaches.[21] In 2018, the mandated self-reports showed this to be true: that year, 120 of the 506 self-reported breaches were snooping incidents. In its 2018 Annual Report, the IPC noted that custodians have increasingly sophisticated and effective methods to detect snooping.[22] The IPC also expressed support for one health care provider's pilot of artificial intelligence

17 2018 Annual Report of the IPC, pp. 24-25.

18 2019 Statistical Report of the IPC, p. 71.

19 2019 Annual Report Downloads, under "Full statistics for 2019," **https://www.ipc.on.ca/2019-annual-report/2019-annual-report-downloads/**.

20 2018 Annual Report of the IPC, p. 31.

21 IPC, "Detecting and Deterring Unauthorized Access to Personal Health Information" (January 2015), **https://www.ipc.on.ca/wp-content/uploads/Resources/Detect_Deter.pdf**.

22 2018 Annual Report of the IPC, p. 24.

technology that can identify possible cases of snooping by detecting and interpreting network activity.[23]

In March 2020, a section on electronic audit logs (section 10.1), was added to *PHIPA*. When this section comes into force, it will require any custodian that uses electronic means to collect, use, disclose, modify, retain or dispose of personal health information to maintain, audit, and monitor an electronic audit log. Among other things, this log must capture the identity of all persons who have electronically viewed a record of personal health information, the type of information that was viewed, and the date and time it was viewed. The custodian must provide the log to the IPC upon request. The IPC welcomed section 10.1 as "a significant step toward strengthened patient privacy."[24]

B. ADMINISTRATIVE PENALTIES

The IPC does not yet have firsthand experience in issuing administrative penalties, but will soon have the ability to issue them. As noted above, provisions were added to *PHIPA* in March 2020 that will allow the IPC to impose administrative penalties.[25] These administrative penalty provisions are in addition to the longstanding "Offences" provision (section 72 of *PHIPA*). Section 72 provides that a person who is convicted of an offence is liable to a fine,[26] but successful prosecutions of offences under *PHIPA* have been rare. Furthermore, the IPC does not lead the prosecution of an offence under *PHIPA*, instead referring the matter to the Attorney General for prosecution. In contrast, administrative penalties offer a more efficient, direct way for the IPC to enforce compliance, without involving the courts.

The administrative penalty provisions fit into the existing structure of the IPC's review and order-making powers. In the existing structure, if the IPC has reasonable grounds to believe—or receives a complaint from someone who has reasonable grounds to believe—that a person has contravened or is about to contravene *PHIPA* or its regulations, the IPC may conduct a review. After conducting such a review, the IPC may make an order directing the person to perform specific actions (e.g., dispose of records collected in contravention of *PHIPA*). In March 2020, the new dimension was added to this order-making power: the power to order the person to pay an administrative penalty if the IPC is of the opinion that the person has contravened *PHIPA* or its

23 2018 Annual Report of the IPC, pp. 26 and 31.

24 IPC Blog, "How government's response to COVID-19 ushered in new privacy protections" (March 31, 2019), **https://www.ipc.on.ca/how-governments-response-to-covid-19-brought-in-new-privacy-protections/**.

25 Bill 188, *Economic and Fiscal Update Act, 2020*, Sched. 6.

26 As of March 25, 2020, the maximum fine for a natural person is $200,000, and the maximum fine for other persons is $1,000,000. Natural persons are also liable to a term of imprisonment of not more than one year, in addition to or instead of a fine. See subsection 72 (2) of *PHIPA*.

regulations.[27] Subsection 61.1 (1) of *PHIPA* states that such an order may be issued for the purposes of (a) encouraging compliance with *PHIPA* and its regulations; or (b) preventing a person from deriving, directly or indirectly, any economic benefit as a result of a contravention of *PHIPA* or its regulations.[28] The remainder of section 61.1 provides further requirements for the order, including the limitation period, the content of the order, and the person to whom payment shall be made.

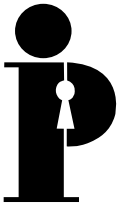
Section 61.1 also provides that the amount of the penalty shall be determined by the IPC in accordance with the regulations made under *PHIPA*. Although *PHIPA* contains this regulation-making authority,[29] the regulations pertaining to administrative penalties have not yet been drafted. Therefore, the IPC does not yet have any direct experience imposing administrative penalties but is preparing itself to do so once the regulations come to pass.

* * *

The IPC appreciates the opportunity to make this submission, and hopes that it serves as helpful background information as the Special Committee conducts its review of *PIPA*.

Patricia Kosseim
Information and Privacy Commissioner of Ontario

27 *PHIPA*, clause 61 (1) (h.1).
28 *PHIPA*, subsection 61.1 (1).
29 *PHIPA*, clause 73 (1) (o.1) and subsection 73 (5).



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

August 2020