2021 *PHIPA* CONNECTIONS SUMMIT

A Conversation with Ontario's Information and Privacy Commissioner

Thank you, Rodney, for your kind introduction, and to the organizers at PSICC for inviting me to speak at this year's *PHIPA* Summit.

The theme of this Summit is *Personal Health Information Management in a Pandemic*, and this pandemic has not only denied us the opportunity to meet in person but has also required us to reschedule this important annual event from its customary December setting to February.

I applaud the nimbleness and creativity with which the organizers have adjusted to this virtual setting and I also appreciate you, the attendees, for adapting to this new normal as well. As with everything else in our lives, this is the new virtual reality we have to roll with nowadays.

As you may know, I started my mandate July 1st of last year, in the middle of the pandemic which was anything but a normal transition. I hit the ground running with a number of issues that required my prompt attention, among them the impact of COVID on access and privacy.

I came to this position with an enormous, long-standing passion for privacy and access issues.

I have had the privilege of working for the federal privacy regulator for many years, but have also worked in the health and health research sectors, for the public sector, the not-for-profit sector, and the private sector, representing clients with many different interests.

I have had the great honor of interacting with very astute practitioners who have a real practical sense of the concrete challenges at play; very smart academics who have devoted their careers to this important field; and very dedicated consumer and civil society groups who play such a vital role in advancing access and privacy rights for the benefit of us all.

If anything, this broad-based experience has taught me to appreciate the many diverse perspectives that come to bear on the complex issues we deal with; it has instilled in me a great sense of humility with which I approach my work and a natural predisposition to listen to others.

Let me kick this off by providing you with **some statistics** from last year as they relate to the health sector.

In 2020, there were **945** *PHIPA* complaints opened with my office. This represents about a **10%** decrease from 2019, where there were **1,038** *PHIPA* complaints opened in that year. While we have not studied the possible reasons for this first time decrease, there is a high possibility that it may be due to decreased visits to health care providers due to the pandemic. For example, according to the Canadian Institute for Health Information, during the pandemic's first wave from March to June 2020, visits to the Emergency Department in Ontario decreased by half and the number of scheduled surgeries were reduced by more than 300,000, as compared to the same period in 2019.[1]

In 2020, there were **194** complaints about access and **180** about privacy. **109** access complaints were dealt with at the mediation stage and **28** health privacy decisions were issued. Only **1** health privacy complaint in 2020 resulted in an investigation.

[1] https://www.cbc.ca/news/health/covid-emergency-department-surgery-cihi-1.5808191

When it comes to privacy **breaches**, there were **528** self-reported privacy breaches in 2020:

105 (or **20%**) were snooping incidents

22 (or **4%**) were ransomware/cyberattacks

And the remaining **401** (or **76%**) were related to:

- lost or stolen personal health information
- misdirected information
- records not properly secured, or
- other collection, use and disclosure issues.

So we can see that snooping, unfortunately, remains a problem -- although with increasing audit trail functionality in computer systems, and the pending requirement for custodians to keep audit logs, which I will speak to soon, I certainly hope to see a reduction in these types of breaches.

Let me now pivot, to give you a **few concrete examples of some significant issues** I have been dealing with since I started my mandate in July.

The very first issue I had to address, quite literally, and urgently awaiting me on my first day was the **COVID Alert app**. As many of you know, this is a voluntary exposure notification app which, unlike a contact tracing app, does not involve the collection of personal information or geolocation information.

Although the app is supported by a federally-developed infrastructure, some aspects are particular to the province or territory in which it is used. For example, in Ontario, these province-specific aspects include how a user receives the validation code that they may enter into the app in the case of a

positive COVID-19 diagnosis, as well as the links the app provides to provincial public health resources.

As Ontario was the first province to launch the app, our office was heavily involved in reviewing its privacy and security features, along with our Federal OPC counterpart.

While the OPC worked with the federal government to review the technical infrastructure and platform, the IPC worked with our government here to review the Ontario-specific features, like how the app interacts with our public health information systems which are subject to oversight by my office.

The Ontario Government consulted with us as they explored options for using smartphone technology for the purposes of exposure notification to help control the spread of COVID-19. We made it clear at the time that, where possible, only non-identifying information should be used to help to control the virus' spread.

We also both worked at our respective ends to influence the negotiations of the Federal-Ontario Memorandum of Understanding to ensure it included strong and robust undertakings on the part of both governments to protect and secure the information gathered from the app. This was especially important knowing that the MOU would likely be used as a template model agreement for other provinces that would eventually get on board.

Our review was based on the Federal/ Provincial/Territorial Joint Privacy principles for contact tracing and similar apps that had been developed in the early months of the pandemic.

While the app is voluntary as it relates to the federal and Ontario governments, there is still a risk that third parties may seek to compel users to disclose information as to their use of the app, including any exposure notifications.

The governments have undertaken to communicate publicly that individuals should not be required to use the app or to disclose information about their use of the app.

The IPC is continuing its oversight to review any changes to the app that may affect its security safeguards and ensure that the app be decommissioned if it is no longer achieving its purpose.

This brings me to another point I want to make clear during these challenging times. During a public health crisis such as this pandemic, **Ontario's privacy laws are not a barrier to sharing information that can help control disease outbreaks**. People need to be told if they have been exposed to the virus so they can take steps to self-isolate or otherwise protect themselves and their families, as well as assess the public health response.

The IPC encourages public health units and other public institutions to provide as much non-identifying information as necessary to help control the spread of the virus and protect public health and safety.

Non-identifying information could include:

- the numbers of affected individuals
- the demographic data such as approximate age and gender
- the geographic locations of infected or deceased individuals
    - this includes schools, long term care facilities, or a workplace
    - or any location where large numbers of people might have gathered.

Organizations that are unsure about Ontario's privacy laws and releasing health information under a pandemic can always call my office.

Another initiative we have been working on is developing **guidance around providing Virtual Care,** which, as this audience knows, is a field that has exploded in large part due to the pandemic.

Debra Grant, the Director of Health Policy here at the IPC, will also be speaking about the recently developed guidance on Virtual Care during her session later this afternoon, but I did want to touch on some key aspects.

First of all, let's get on the same page when we speak about Virtual Care. What do we mean by that term? Well, virtual care can include:

- Email messages/photos
- Telephone consultations
- Live videoconferencing
- As well as newer and emerging technologies such as
    - post-acute care remote monitoring,
    - patient portals,
    - wearable devices, and
    - health-related apps.

We must remember that *PHIPA* applies to virtual care as it does to in-person care. This new and expanding digital world raises key privacy and security concerns:

- The potential for interception by an unauthorized third party, or
- Inadvertent misdirection which may result in the unauthorized disclosure of personal health information.

It is imperative that custodians take reasonable steps to have virtual care safeguards in place. For example, custodians should have a written virtual care policy that:

- Addresses when /how care may be provided virtually
- The conditions or restrictions for providing care virtually, and
- Sets out the administrative, technical and physical safeguards.

Custodians should always apply the “principle of least privilege”: this means that agents only have access to the minimum amount of personal health information required when engaging with virtual care technologies to perform their job duties. This aligns with data minimization principles under *PHIPA*.

Comprehensive privacy and security training is essential for reducing the risk of unauthorized collection, use and disclosure of personal health information.

In addition, custodians are expected to have a privacy breach management protocol in place that identifies the reporting, containment, notification, investigation and remediation of actual and suspected privacy breaches.

The IPC has guidance on our website entitled *Responding to a Health Privacy Breach: Guidelines for the Health Sector*.

Another important aspect of virtual care involves strong security preferences and passwords, data encryption and the secure storage of the data.

Custodians need to be asking themselves - who has access to the data?

Custodians need to ensure data sharing agreements are in place when using wearables or apps.

And custodians should urge caution when recommending the use of wearables or apps to patients – due diligence is required.

With respect to **videoconferencing**, for example, steps should be taken to protect the privacy and security of the information when planning and preparing for a meeting as well as during the meeting.

Planning and preparation involves ensuring a videoconferencing tool/platform with sufficient security safeguards, a secure connection, and a private location. As part of planning, custodians should determine if videoconferencing is the appropriate method to provide health care:

- Will the provider be able to meet the necessary standard of care?
- Will the provider be able to uphold their obligation to protect the privacy of the patient's personal health information?

And during the meeting, if others are present, the patient must consent to their presence during the virtual visit.

It is also important to communicate a back-up plan in case the video connection fails.

And custodians should always be aware of any policies the applicable regulatory college has published (for example, the College of Physicians and Surgeons of Ontario's Telemedicine policy), as well as other resources, such as the Ontario Telemedicine Network's *Privacy Toolkit*.

And prepare to consider how the regulations, once made, regarding:

- consumer electronic service providers and
- interoperability specifications
- might apply to the virtual provision of health care.

Debra Grant will speak in more depth to the issue of virtual care, and more details are provided in our guidance which is available

on our website and I invite you to read. But as you can see, this is a complex and fascinating topic that will continue to challenge us in the future.

Let me now take a minute to discuss one of the province's initiatives to address the pandemic. This is the Ontario Health Data Platform (OHDP), which is being developed by the Ministry of Health. The Ministry states that "OHDP links large health datasets from a variety of sources to create an unprecedented volume of rich, connected data." Researchers can use these datasets in an effort to better detect, plan, and respond to COVID-19 and its effects. Researchers who seek access to the OHDP must first apply and go through a screening and approval process.

Also, governance structures have been developed; this includes the appointment of Dr. Jane Philpott as the Special Advisor and Chair of the Joint Ministers' Roundtable for the OHDP. Here is some important backstory on how the OHDP was created.

Back in the spring of 2020, when the Ministry was formulating its plans for the OHDP, the Ministry determined that the province did not have easily accessible datasets in one repository with the capacity required for high performance computing and fine-grained analysis. As such, the Ministry proposed an amendment to the Regulation under *PHIPA* in order to enable the OHDP.

When the proposed amendment was publicly posted, the IPC made the following recommendations:

- That the Ministry place a time limit on the permitted disclosures in the regulation;
- That the Ministry require that the personal health information collected be securely disposed of or de-identified when the regulation expires;

- That the disclosure of personal health information to the platform uphold principles of necessity and proportionality;
- That the OHDP provide the people of Ontario with information regarding the platform; and
- That the Ministry ensure appropriate oversight and accountability to the people of Ontario.

Underlying our recommendations is the fact our office recognizes both the importance of making COVID-19 data available to researchers and the importance of protecting the privacy of individuals and the security of their information.

On July 30, 2020, the regulatory amendment was made. It states that ICES and Ontario Health (which are two of the prescribed entities under *PHIPA*) are required, upon request of the Minister of Health, to disclose personal health information to the Minister where the Minister has determined that such disclosure is necessary for the purposes of:

- researching, analyzing, investigating, preventing, responding to or alleviating COVID-19 or its effects; or
- evaluating or monitoring the impact of COVID-19 on the management of, the allocation of resources to or planning for all or part of the health system.

The amendment is set to expire on July 30, 2022.

The OHDP is still in its final stages of development and my office continues to engage in consultations with the Ministry and the OHDP on privacy and security implications about this important big data platform as it ramps up to contribute to COVID-related research in the province.

Finally, another area I want to go over with you today, involves the **recent changes to *PHIPA* and its Regulation**.

Since 2019, the Ministry of Health has been seeking to modernize *PHIPA*.

This process has resulted in amendments to *PHIPA* in:

- Bill 138, *Plan to Build Ontario Together Act, 2019*
- Bill 188, *Economic and Fiscal Update Act, 2020*

Some amendments are currently in force and others are not.

Let's discuss a few of the changes.

First, I want to discuss Bill 188 and its introduction of **Administrative Penalties**. Ontario is the first jurisdiction in Canada to have this power.

Bill 188 added to *PHIPA* the ability for the IPC to issue administrative penalties for the purposes of encouraging compliance with *PHIPA* and its regulation, or preventing a person from deriving, directly or indirectly, any economic benefit as a result of a contravention of *PHIPA* or its regulation.

What does this mean? It means that my office will be able to impose administrative monetary penalties directly against persons who contravene *PHIPA*. The penalty amounts and their administration have yet to be determined by regulation.

The administrative penalty provisions fit into the existing structure of the IPC's review and order-making powers which authorize the IPC to make an order directing a person to perform specific actions (for example, to dispose of records collected in contravention of *PHIPA*).

In contrast to the "Offences" provisions under *PHIPA*, administrative penalties will offer a more efficient, direct way for the IPC to enforce compliance, without involving the courts.

Though the amendment is in force, administrative penalties cannot be issued until a regulation is made.

To be clear, the administrative penalty framework will exist separately from the long-standing “Offences” provisions of *PHIPA*, found in section 72. Section 72 provides that a person who is convicted of an offence is liable to a fine. However, 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.

But with respect to the Offences provisions, another Bill 188 amendment has established harsher consequences for being convicted of an offence under *PHIPA*. The maximum fine upon conviction for a natural person is now $200,000, and the maximum fine for other persons is $1,000,000. Natural persons are also now liable to a term of imprisonment of not more than one year.

Another amendment addresses the increasing concern about the ability of organizations to use large data sets of de-identified health information to re-identify individuals.

In light of these concerns, three amendments were made to *PHIPA* to **regulate de-identified information:**

1. Bill 138 amended *PHIPA* to prohibit a person from using or attempting to use de-identified information to identify an individual, subject to certain exceptions (in force as of July 31, 2020)

2. Bill 138 also created an offence for willfully contravening this prohibition on the use of de-identified information to re-identify an individual (in force as of July 31, 2020) and

3. Bill 188 amended the definition of “de-identify” to enable requirements to be prescribed for how personal health information is to be de-identified.

As I have discussed in my blog, along with the new teeth *PHIPA* now has with the administrative penalties and enhanced offence fines, Bill 188 also ushered in new rights and responsibilities.

Since before the pandemic, the Ontario government has been working to modernize *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 increasingly share individuals’ personal health information with one another in order to deliver care in a coordinated and effective manner.

With the increase in electronic forms of communication, there was a concern that an individual’s right of access under *PHIPA* would become outdated. Individuals are also increasingly taking steps to manage their own health information through patient portals and health apps. The Ontario government has been working to modernize *PHIPA* to account for the fact that personal health information is collected, used and disclosed in an **increasingly digital format.**

In light of these changes, two amendments were made to *PHIPA*:

1. Bill 188 amended *PHIPA* to give individuals the **right to access their records of personal health information in an electronic format** (pursuant to regulations to be prescribed) so they could take steps to manage their own health information, including potentially through patient portals and health apps; and

2. Bill 188 also amended *PHIPA* to regulate a new class of persons called **“consumer electronic service providers”**

(CESPs) to provide for responsibilities for the providers of these patient portals and digital health apps (the CESPs) to comply with certain requirements that have yet to be defined in regulations.

The services that CESPs provide are primarily for allowing consumers to access, use, disclose, modify, maintain or otherwise manage their records of personal health information. Apps are the typical example.

The IPC has the power to make an order requiring a health information custodian or a class of health information custodians to cease providing personal health information to a CESP.

Also, the bill sets out explicit requirements for all custodians to maintain and monitor an **electronic audit log** of all instances where personal health information is viewed, handled, modified, or otherwise dealt with, and to provide a copy of this log to my office on request.

I believe that electronic audit logs are an important tool to detect and deter unauthorized access to personal health information.

This obligation flows from the requirement in *PHIPA* for custodians to take reasonable steps to protect personal health information, for example, against theft, loss and unauthorized use or disclosure.

There is an increasing concern that personal health information in electronic form cannot be easily communicated between electronic systems (e.g. hospital information systems, electronic medical records).

To address this concern, Bill 138 amended *PHIPA* to add regulation-making authorities governing **electronic interoperability requirements.** Interoperability helps ensure that

custodians' electronic information systems, or "digital assets," can "speak to one another" making it easier for custodians to share PHI seamlessly across institutions.

New regulations under *PHIPA* came into force on January 1, 2021 that require Ontario Health to make and publish interoperability specifications relating to these digital assets, in consultation with my office (particularly where individuals' privacy and access rights are at issue). These interoperability specifications are subject to approval by the Minister of Health.

Ontario Health is also required to develop a certification process to green light the digital assets that meet the required specifications.

Vendors of digital assets will be affected indirectly: if they are developing a digital asset that they hope Ontario custodians will use, they know that such an asset must comply with applicable interoperability specifications.

Custodians, for their part, will be required to ensure that their digital assets comply with the applicable interoperability specifications. Ontario Health has the ability to monitor compliance.

If a custodian does not comply, this regulation would be enforced through a complaint to the IPC.

Now I want to finish off with a few words about the long-awaited **Electronic Health Record (EHR).**

On October 1, 2020, new regulations designated Ontario Health as the prescribed organization responsible for the province's EHR under Part V.1 of *PHIPA*. One of the main goals of the EHR is to ensure that Ontarians' comprehensive health information is brought together in a consistent format under a single, virtual

'roof.' This will make the information readily accessible to a broad range of health care providers across a wide spectrum of care settings, enabling more efficient and better-integrated care.

I discuss this on my December 3rd blogpost entitled *Incremental but consequential: 2020 changes to PHIPA*, which you can reference on the IPC website. But I think it is important to go over the main points.

Part V.1 establishes a comprehensive privacy and accountability framework for the EHR. It defines an extensive role for Ontario Health as the administrator of the EHR subject to oversight by my office.

It allocates shared responsibilities among multiple custodians using the EHR, to establish "who's on first." For example, it clarifies the rules for custodians seeking to upload or download PHI, to or from the EHR; rules for honoring an individual's consent directives and rules for overriding them, subject to notice requirements.

There are also new rules for breach notification adapted specifically for the EHR context. Regulations prescribing when my office must be notified of unauthorized collections from the EHR came into force October 1, 2020. There are additional notification and reporting obligations for custodians.

- The IPC must be notified of an unauthorized collection from the EHR in the same circumstances as if the collection were an unauthorized use or disclosure outside of the EHR.
- The IPC must be notified of all consent overrides for the purpose of eliminating or reducing a signification risk of serious bodily harm to a person other than the individual to whom the information relates or a group of persons.

It is important to remember that, even if you do not need to notify the IPC, you have a separate duty to notify individuals of breaches under sections 12(2) and 55.5(7)(a) of *PHIPA*.

And individuals must also be notified of all consent overrides (collections and uses contrary to a consent directive) in the EHR.

There are new rules that allow coroners, medical officers of health, and the ministry of health's data integration unit (designated under Part III.1 of FIPPA) to collect PHI from the EHR. The Minister of Health may also direct disclosure of PHI from the EHR to others (for example, researchers) on request, subject to consultation with a yet-to-be- established advisory committee. This concept of an advisory committee is yet another interesting aspect of *PHIPA*.

So, those are just a few of the exciting new developments that have happened over this past year, and what a year it has been. I am looking forward to meeting the challenges that lay before us in 2021 and continuing to serve the people of Ontario, ensuring the right to privacy and access.

Thank you for listening and I believe that Rodney and I are going to have a little virtual fireside chat now.