

PROTECTING PRIVACY IN A PANDEMIC

INTERPRETING *PHIPA* IN LIGHT OF COVID-19

As the impact of the novel coronavirus (COVID-19) pandemic continues to grow worldwide, a key challenge that emerges for health professionals is the question of how to respond to the demands of a public health emergency while ensuring the continued protection and privacy of the personal health information of individual patients.

In Ontario, the *Personal Health Information Protection Act, 2004* (“*PHIPA*”)¹ broadly governs and protects the collection, use and disclosure of personal health information by health information custodians (a definition which includes regulated health professionals). Importantly, even in circumstances of a public health emergency, such as COVID-19, *PHIPA* continues to apply and place obligations upon regulated health professionals. However, *PHIPA* does not clearly outline specific obligations that apply in relation to a public health emergency. As such, the question becomes – how should health professionals interpret and apply their obligations under *PHIPA* in these circumstances?

The Information and Privacy Commissioner of Ontario (“*IPCO*”) has not yet released specific guidance on how to interpret *PHIPA* provisions during a public health emergency such as COVID-19. As such, health professionals should be encouraged to look to other sources for assistance in clarifying their obligations under *PHIPA*.

What is “Substantially Similar” Privacy Legislation and Why is it Helpful in Relation to COVID-19?

At the federal level, the *Personal Information Protection and Electronic Documents Act* (“*PIPEDA*”)² narrowly governs the collection, use and disclosure of

personal information by private-sector organizations during the course of “commercial” activity in Canada. However, this piece of legislation also sets out the general standard or model for privacy protection across Canada. In cases where the Governor in Council deems that provincial/territorial privacy legislation has met the standards for privacy protection set by *PIPEDA*, it may deem the legislation to be “substantially similar” to *PIPEDA*.

Namely, “substantially similar” provincial/territorial laws:

1. Provide privacy protection that is consistent with and equivalent to that found under *PIPEDA*;
2. Incorporate the ten fair information principles for the collection, use and disclosure of personal information listed in Schedule 1 of *PIPEDA* (*i.e.* accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance);
3. Provide for an independent and effective oversight and redress mechanism with powers to investigate; and
4. Restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.³

In the context of personal health information, Ontario’s *PHIPA* has been deemed “substantially similar” legislation to *PIPEDA*. This is important for

¹ S.O. 2004, c. 3, Sched. A.

² S.C. 2000, c. 5.

³ <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic->

[documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/)

health professionals to understand because it means that, where guidance is lacking from the IPCO in relation to a particular health issue, they should consider any available and relevant guidance from the federal Privacy Commissioner in relation to *PIPEDA*.

Health professionals can also consult guidance documents from other provinces/territories with “substantially similar” health privacy legislation. To date, this includes the provinces of Nova Scotia, Newfoundland and Labrador, and New Brunswick.

COVID-19 Guidance from Substantially Similar Legislation

Accordingly, in relation to COVID-19, the federal Privacy Commissioner has released helpful guidance that health professionals should consider and apply when collecting, using and disclosing personal health information under *PHIPA*.

Drawing from the provisions of *PIPEDA*, the federal Privacy Commissioner reminds organizations of the following general principles that are particularly applicable in the context of a public health emergency:

- Collection, use and/or disclosure of personal information should **only** be done for purposes that a **reasonable person would consider appropriate in the circumstances**;
- The individual’s knowledge and meaningful consent **must** be obtained for the collection, use or disclosure of their personal information; and
- Consent is only valid where it is reasonable to expect that the individual **understands the nature, purpose and consequences of the collection, use and/or disclosure of the personal information to which they are consenting**.⁴

However, recognizing that, in the context of a public health emergency, obtaining consent from an individual can be particularly difficult, the federal Privacy Commissioner also highlights the following circumstances under *PIPEDA* in which organizations may collect, use and/or disclose personal information

without an individual’s consent. These include circumstances where:

- The collection is clearly in the interests of the individual and consent cannot be obtained in a timely way. This includes, for example, circumstances where an individual is critically ill or in a particularly dangerous situation requiring assistance.
- The collection and/or use of the personal information is done to comply with a disclosure that is required by law. This includes, for example, circumstances where a public health authority (acting under law) requires that the information be disclosed.
- A government institution (*e.g.* a public health authority) acting under law, requests disclosure of the personal information for the purpose of enforcing or administering federal/provincial/territorial laws.
- The organization initiates disclosure of the personal information to a government institution because it has reasonable grounds to believe that the information relates to a contravention of federal/provincial/territorial laws. This includes, for example, circumstances where an organization believes that an individual is contravening an invoked quarantine order.
- Disclosure is necessary for the purpose of acting in response to an emergency that threatens the life, health or security of an individual. This includes, for example, circumstances where an individual requires urgent medical attention but cannot communicate directly with health professionals.

For further assistance interpreting specific provisions under *PHIPA*, along with guidance relating to specific COVID-19 related scenarios, health professionals can also consult guidance released from the Office of the Information and Privacy Commissioner of Newfoundland and Labrador (available [here](#)).

⁴ https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/