

April 22, 2020

## ARTICLE

# COVID-19 privacy considerations for Ontario's health care sector

Overview: What is the impact of COVID-19 on privacy/access rules?

Transparency and quick information flow are essential during a public health emergency, and privacy rules may be viewed as a barrier to health providers doing their job. That said, the *Personal Health Information and Protection Act* (PHIPA) remains in force during the COVID-19 pandemic, and its provisions are in large part sufficiently flexible to allow health information custodians and their employees to do their jobs during the pandemic. Most importantly, Ontario's privacy rules provide for the disclosure of COVID-19 information to public health authorities and to others facing a risk of serious harm caused by COVID-19.

The time limits for responding to access requests remain in force during COVID-19. However, the Information and Privacy Commissioner of Ontario (IPC) has warned requesters to expect delays and has indicated that organisations should "make reasonable efforts, *based on operational realities*, to comply with Ontario's access laws."

## 1. IPC acknowledges that different standards apply in exceptional circumstances

In a statement released on March 16, 2020, [Impact of COVID-19](#) (IPC Statement), the IPC provides the following guidance:

- These are exceptional circumstances and it may not be possible for organisations to meet the same standards for security and privacy protection that they normally do. Many organizations are striving to manage service disruptions and to continue to provide essential services, especially in the health sector.
- Where required, staff (or agents) can be allowed to handle personal health information (PHI) from home, in order to provide necessary services in an effective and efficient way. Organisations should guide staff working from home on how to do their work within as privacy-protective an environment as they can, given the realities of the current situation.
- In a public health crisis, it is also understandable that health care professionals may need to send or receive information by phone, text, email or other messaging services. This applies to the use of technologies not normally used for business, during this crisis.

## 2. Security standards during COVID-19

PHIPA provides that custodians "shall take steps that are reasonable in the circumstances" to protect PHI against theft, loss and unauthorized use or disclosure. As the IPC Statement suggests, what constitutes reasonable steps during COVID-19 may be different from normal times. While security standards may be relaxed during COVID-19, custodians should nonetheless promote practices that reduce risks to patient privacy.

### *Practical tips*

The IPC Statement provides practical tips to protect privacy when staff are working from home. We have adapted that list and added to it to reflect the realities of the health care sector:

#### Mobile devices

- Encourage staff to password-protect their devices and use auto-locking features.
- If possible, use portable storage devices, such as USBs and portable hard drives that are encrypted and password protected.
- Encourage staff to keep software up-to-date.

#### Communication

- Encourage staff to continue to avoid discussing PHI in public areas.
- Advise staff to use work email accounts rather than personal ones for work-related purposes.
- Consider adopting an enterprise texting solution that facilitate team communication in a secure manner.

#### Paper files

- If new treatment areas or premises are established, set up file storage in areas only accessible to staff and equip them with locked cabinets, and ensure that records that do not need to be maintained can be securely disposed of.
- Encourage staff to bring paper files home only if necessary, and to keep them in a safe place and not in their car.

#### Cyber risk

- Warn staff about the heightened risk of cyberattacks, including phishing emails purportedly related to COVID-19.
- Ensure that all temporary or off-site networks are secure.

- Encourage staff to inform you about the new apps and technologies they are using so that their risks can be assessed by IT departments.

## Breach Notification during COVID-19

PHIPA requires custodians to notify individuals of any loss, theft or unauthorized use or disclosure of their PHI at the "first reasonable opportunity". Again, what this means during COVID-19 is likely different than in normal times, and delays in privacy breach notification to individuals are to be expected.

There is no legislated timeline for breach reporting to the IPC. The IPC's office is closed and only a limited number of staff are providing essential services until the office reopens. In that context, it is reasonable to delay breach reporting to the IPC until COVID-19 is over unless circumstances are exceptional.

### *Practical tips*

- Prioritize the notification of individuals when there is a reasonable risk that the privacy breach will cause harm to them (e.g., identify theft or fraud).
- If a breach affects a significant number of individuals, seek legal advice.
- Leave notification in other cases to when circumstances will allow.

## 3. Disclosure of COVID-19 status

Ontario's *Health Protection and Promotion Act* (HPPA) requires health care providers to report to a Medical Officer of Health of the local health unit that an inpatient or outpatient has or may have COVID-19. Regulation 569 under HPPA specifies what information should be included in such a report.

In addition, PHIPA provides that a custodian may disclose PHI to a Medical Officer of Health or to Public Health Ontario (or to a public health authority in another jurisdiction) if the disclosure is made for the purposes of HPPA. The purpose of HPPA include "the prevention of the spread of disease and the promotion and protection of the health of the people of Ontario."

PHIPA also allows for the disclosure of COVID-19-related information to persons other than public health authorities in certain circumstances. A custodian may disclose PHI if there are reasonable grounds to believe the disclosure is necessary to eliminate or reduce a significant risk of serious harm to individuals. The spread of COVID-19 poses a significant risk of serious harm, and, as such, a custodian can rely on this provision to notify staff or patients that they have been in close contact with an individual who has COVID-19 symptoms or has tested positive. Organizations should limit the disclosure to what is necessary in the situation and, where possible, avoid revealing the identity of the individual affected or potentially affected by COVID-19.

On April 3, 2020, Ontario ordered new emergency measures requiring laboratories, including laboratories operated by hospitals, to disclose COVID-19 status information to first responders authorized to request that information. The goal is to allow first responders, notably police, firefighters and paramedics, to take appropriate safety precautions to protect themselves and the community. COVID-19 status information is limited to the individual's name, address, date of birth, and whether the individual has had a positive COVID-19 test result. The order also contemplates the disclosure of COVID-19 status information to the Ministry of Health if it develops a system for sharing this information among first responders.

## 4. Flow of PHI between care providers

Custodians have the implied consent of their patients to disclose PHI to other custodians for the purpose of providing or assisting in providing health care. This means custodians can disclose PHI to a physician's office, pharmacy, long-term care or retirement home, home care service provider, ambulance service, and laboratory without obtaining express consent. For example, the [CPSO COVID-19](#) FAQs clarifies that physicians are permitted to share information about a patient's COVID-19 status with a pharmacist involved in the patient's care. The CPSO notes that "[s]haring this information enables the pharmacist and patient to coordinate for delivery of the medication or alternative pick-up by a family member, friend, etc."

PHIPA allows a hospital to use PHI for the planning or delivering of programs or services, allocation of resources, and evaluation and monitoring. However, it does not currently allow a custodian to disclose PHI for such purposes, unless the disclosure is to a prescribed entity (e.g., CCO, CCSO, CorHealth). Where there is a barrier to the sharing of information between custodians and non-custodians working together to respond to COVID-19, written agreements may be able to resolve the issues.

### *Practical tips*

- If possible, enter into written agreements with new partners that set out the relationship between the parties and their obligations regarding privacy and PHI.

## 5. Immunity under PHIPA

Care providers and health care organizations should strive to uphold the privacy of their patients' information. However, it is important to note that PHIPA provides immunity to custodians and their agents exercising (or intending to exercise) powers and duties under PHIPA for good faith acts or omissions that were reasonable in the circumstances. This immunity has received very little judicial consideration. It may very well apply where PHIPA is contravened in the course of trying to stop the spread of COVID-19.

## 6. Access/correction requests under PHIPA and FIPPA

Individuals and the media may want access to information in connection with COVID-19. At the same time, hospitals focused on responding to COVID-19 and managing the front lines may not have the operational capacities to respond to access requests.

Regulation 73/20 made under the *Emergency Management and Civil Protection Act* (EMCPA) suspends the application of periods of time within which any step must be taken in any proceeding in Ontario, including an intended proceeding. Regulation 73/20 applies to proceedings before the IPC, including appeals of decisions made under access laws. However, Regulation 73/20 does not suspend the period for responding to an access request under PHIPA and the *Freedom of Information and Protection of Privacy Act* (FIPPA).

A hospital has 30 days to make a decision with respect to an access request under FIPPA/PHIPA. Hospitals can extend this time limit where the records requested are voluminous or external consultations are required. While FIPPA/PHIPA do not allow extensions due to disasters or public health emergencies, the IPC Statement warns individuals making access request to anticipate delays during COVID-19. The IPC Statement also indicates that the IPC expects organizations to "make reasonable efforts, based on operational realities, to comply with Ontario's access laws. However, this is an exceptional circumstance and we understand that many organizations will be unable to meet the 30-day response requirement."

Where a hospital cannot deal with a request within the required time, the request will be deemed to have been denied. The IPC Statement indicates that the IPC will "consider [COVID-19] circumstances when evaluating appeals relating to deemed refusals."

### *Practical tips*

If your organization does not have the operational capacity to handle all FIPPA/PHIPA access requests, consider:

- Prioritizing PHIPA requests made for the purpose of accessing health care services or necessary benefits over those made in connection with existing legal proceedings, which are currently on hold because of COVID-19.
- Prioritizing FIPPA requests that relate to COVID-19 over requests that deal with matters that are historic and/or unlikely to be of broad public interest.
- Informing requesters that you may be unable to consider the request within 30 days due to COVID-19 and that the request will be processed as soon as circumstances allow.

---

By: [Daniel Girlando](#)

Services: [Disputes](#), [Health Care](#), [Patient Care](#), [Personal Health Information & Privacy](#)


---

## Related Contacts

Patrick J. Hawkins  
Partner

 Toronto


 [PHawkins@blg.com](mailto:PHawkins@blg.com)

 [416.367.6065](tel:416.367.6065)

Allison Foord  
Partner

 Vancouver

 [AFoord@blg.com](mailto:AFoord@blg.com)

 [604.640.4079](tel:604.640.4079)