SAFEGUARD

A quarterly newsletter published by the Office of the Information and Privacy Commissioner

Volume 4, Issue 3 August, 2020

Contact Information

Office of the Information and Privacy Commissioner

3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8

Telephone:

709-729-6309

Fax:

709-729-6500

Toll Free in Newfoundland and Labrador:

1-877-729-6309

Email:

commissioner@oipc.nl.ca

www.oipc.nl.ca

This Issue:

How has *PHIA* Fared during the Pandemic?

As of June 25, 2020, Newfoundland and Labrador is at Alert Level 2 under the province's COVID-19 Alert System and many businesses, public bodies and health care providers have largely returned to something approaching normal operations. This includes the Office of the Information and Privacy Commissioner (OIPC). The past five months have held numerous hardships for those working in the health care field with the extra stress of providing care in the context of a pandemic and usual operations disrupted. COVID-19 testing, contact tracing, and developing new policies and procedures for remote consultations with patients, among other complications, have greatly added to the workload of many health care providers.

COVID-19-Related Privacy Breaches

Responding to a major public health emergency such as COVID-19 requires a careful and at times difficult balancing of the protection of personal privacy with ensuring that custodians and public health authorities are sharing necessary information with each other and the public. Immediately prior to the declaration of the public health emergency our Office released "Don't Blame Privacy – What to Do and How to Communicate in an Emergency" to help guide custodians and public bodies in the handling of personal information and personal health information.

There are many ways privacy may be impacted during a pandemic: contact tracing efforts may require the collection of personal information and personal health information; custodians may be relying more on fax or electronic communications to avoid contact between staff or reduce foot-traffic within hospitals; anxiety about the spread of COVID-19 may prompt custodians or staff to improperly seek out information about patients and test results. Since March, 18, seven breaches related to COVID-19 have been reported by custodians and

public bodies under both the *Access to Information and Privacy Act, 2015* (*ATIPPA, 2015*) and the *Personal Health Information Act* (*PHIA*). However, these represent less than 10% of the more than 70 breaches reported since that date. Any privacy breach is serious but this Office is thankful that the pandemic has not resulted in more breaches.

New *PHIA* Prosecution

In June, 2020, the OIPC laid charges under *PHIA* against a former employee of Central Health in connection with unauthorized access to the records of personal health information of one individual. The matter is set for a first appearance in October, 2020. This Office is gratified by the complete cooperation and assistance we have received from Central Health in our investigation of this matter.

Under section 88 of *PHIA*, it is an offence for a person to falsely obtain (or attempt to obtain) another person's personal health information; to make false statements to, or obstruct the work of, the OIPC or another person performing duties under *PHIA*; or to destroy personal health information with the intent to evade a request for that information. Further, it is an offence for a custodian or information manager to collect, use, or disclose personal health information contrary to *PHIA*; to fail to protect personal health information; or to disclose personal health information for a monetary or other benefit.

Those found guilty of an offence under *PHIA* are liable to a fine of up to $10,000 or a prison term of up to six months.

PHIA and Virtual Medicine

In light of the COVID-19 pandemic, interest in the provision of health care through virtual platforms or apps has increased greatly. However, moving health care and the exchange of personal health information into the virtual realm is not without risks.

One example of the risks of providing virtual health care is the experience of UK-based health service provider Babylon Health. Babylon Health (which has a presence in Alberta, where it is partnered with Telus) provides remote consultations with doctors and health care professionals via text and video messaging through a mobile app. In June, 2020, several UK-based users of the Babylon Health app discovered that they were able to access video recordings of consultations between doctors and other patients. Babylon Health was advised of the breach and determined that it was the result of technical error rather than an intentional attack on their system.

The rising use of virtual platforms, and the example of Babylon Health, presents several questions about how personal health information is handled when an individual interacts with their health care provider in this manner. Does privacy legislation, such as Newfoundland and Labrador's *PHIA* apply? Who is responsible if there is a breach of your privacy?

The duty to protect personal health information is imposed on "custodians", who are defined at section 4 and include health care professionals (including physicians, dentists, nurses and similar professions), health care providers, regional health authorities, the Department of Health and Community Services, and others. Such custodians have a duty to protect personal health information in their possession. Personal health information includes not only traditional medical

records, consultation notes, test results, prescriptions or referrals, but also any video or audio recorded and stored by the virtual platform.

In the case of responsibility for protecting personal health information when health care has been provided through some virtual platform, the physician providing the health care services would be the custodian of any personal health information shared through, or stored on, the platform.

Just as would be expected when providing in-person services, physicians providing care through a virtual platform have a duty to take reasonable steps to maintain proper safeguards to protect the personal health information of their patients which may be shared through the platform. This would include any information the patient provides to the platform, as the patient will be considered to have provided that information to their physician, the custodian under *PHIA*.

The virtual platform itself is accounted for in *PHIA* as an information manager (see section 22). While information managers are required to comply with *PHIA* and ensure the protection of any personal health information in their custody, the custodian – the physician or other health care professional or provider – actually providing care ultimately remains responsible for compliance with *PHIA*. As a result, any privacy breach – such as that experienced by Babylon Health – could generate liability for both the custodian and the information manager.

Should a privacy breach occur on a virtual health care platform, the platform provider (being an information manager) must notify the custodian(s) as soon as practicable. Subject to some exceptions at section 15 of *PHIA*, the custodian is then responsible for notifying this Office and those individuals whose personal health information is the subject of the breach. Privacy breach notification forms can be found on our website.

Once in receipt of a breach notification, the OIPC will consider whether the custodian and, by extension, the information manager, took reasonable steps to ensure the security of personal health information. We will look at, among other things: the information management agreement between the custodian and the information manager; security measures employed; policies and procedures; and training. Based on our review of a privacy breach, the Commissioner may elect to conduct an own-motion investigation.

If the virtual health care platform transfers or ultimately stores personal information or health information outside of Newfoundland and Labrador, the protection of that information may, in addition to *PHIA*, also be subject to the laws of the jurisdiction where that data is ultimately transferred or stored, including the federal *Personal Information Protection and Electronic Documents Act*. If information is transferred outside of Canada, other legislation may also apply based on where the information is ultimately transferred.

Virtual health care platforms, including the use of video and audio to facilitate remote consultations, present an attractive opportunity to reduce barriers to accessing health care and to protect health care workers and vulnerable populations in the midst of a pandemic. However, there are risks, and physicians and other custodians must be aware that they ultimately bear the onus of protecting personal health information and that they must take all reasonable steps to do so. Before partnering with virtual health care platforms or other information managers, physicians should ensure that they understand how the system works and develop policies and practices to mitigate risk.

Decision in Joint Ontario and British Columbia LifeLabs Investigation

On June 25, the Ontario IPC and BC OIPC announced the findings of their investigation into the company's 2019 data breach, concluding that LifeLabs failed to take reasonable steps to protect personal health information; failed to have adequate information technology security policies in place; and collected more personal health information than was reasonably necessary.

The full report is not yet available as LifeLabs has sought a court order against its release, on the basis that it contains privileged information. However, on July 29, the company did advise that it will comply with all of the Commissioners' orders and recommendations.

Email Breaches

Emails are a common source of inadvertent breaches reported to our Office. Incorrectly entered email addresses, or emails that have gone to another person with the same name as the intended recipient, risk breaching the privacy of personal health information.

Often, if the error is discovered early on, custodians and public bodies have reported their efforts to "recall" an email through Outlook. However, employees should be aware that there are shortcomings in Outlook's recall function and it should not be relied on to protect against breaches. A message can only be recalled within the same organization; recall will not work if the recipient is using Outlook Web App ("OWA") webmail or if they are not connected to the network; and, perhaps it goes without saying, recall will not work if the message has already been read.

The following are steps that employees can take to reduce or prevent email-related breaches.

- Turn off Outlook's Auto-Complete address feature under File > Options > Mail > Send Messages; this can prevent you from sending an email to a recipient with a similar name.
- Use your address book to populate To, Cc and Bcc fields.
- Instead of composing a new message, reply to a previous email from the intended recipient.
- Delay the delivery of emails through Outlook's Rules & Alerts. An extra two minutes spent in the Outbox might be enough to realize a mistake and catch an error before it is sent.

PHIA Statutory Review

On July 27, the Government of Newfoundland and Labrador announced its *ATIPPA, 2015* review. Previously, in November 2016, the statutory review of *PHIA* was announced. Many stakeholders expended significant time and effort in contributing to the review process, as did the review committee, chaired by Dr. David Morgan. The *PHIA* Statutory Review Committee's final report was published in May 2017.

No legislative changes have yet been announced as a result of this comprehensive review, however the OIPC looks forward to this important item being actioned by government in the near future. The 2017 *PHIA* Review Report is available at http://www.phiareviewnl.ca.