



SAFEGUARD

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

Volume 4, Issue 4

November 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

In This Issue:

- COVID Exposure Alert App
- Virtual Healthcare
- Review of Recent Decisions and Reports
- Complaints and Breach Notifications

COVID Exposure Alert App

In September, the Office of the Information and Privacy Commissioner (OIPC) concluded our review of the COVID Alert exposure notification application and extended our support for use of the app. Although the federal government led the development, the Privacy Commissioner of Canada and the Ontario Information and Privacy Commissioner ensured that privacy commissioners across Canada were consulted. Its development is consistent with the privacy principles expressed by federal, provincial, and territorial privacy commissioners in a May 2020 [joint statement](#). The resulting app was developed based on a protocol developed by Google and Apple and, while it leverages federal work, the version launched here has been customized for this province.

The app is based on a protocol that does not involve the collection of personal information by the government or any company, as the technology has been designed to ensure the data is anonymized. It has been subject to scrutiny by privacy and cybersecurity experts around the world. The app demonstrates that modern technology can meet an emerging need without the mass collection of personal information.

Downloading and using the app must be entirely voluntary. This is an important civil liberties issue. The OIPC encourages the provincial government to consider enacting legislation to prohibit anyone, public or private, from requiring use of the app as a condition for the provision of goods, services, entry into a premises or facility, or into the province itself.

The OIPC expects the Department of Health and Community Services to evaluate adoption and implementation of the app to ensure that it functions as intended and continues to meet the identified need.

For updates relating to the COVID Exposure Alert App, including number of downloads and updated listed of provinces and territories making use of the app, please visit the [official application website](#).

Virtual Healthcare

At the start of 2020, few could have predicted a global health pandemic or the rapid changes that such an illness would have on the world. COVID-19 has certainly accelerated changes in the health sector, from the transition to virtual and phone appointments to the implementation of COVID-19 screening questionnaires. The pandemic has create an opportunity for not just digital solutions, but digital transformations. However, what impact do these opportunities have on a custodian's compliance with the *Personal Health Information Act (PHIA)*?

The health sector has experienced a change in demand as well in its service-delivery model since the declaration of a public health emergency in March 2020. As we settle into this “new normal”, we have an opportunity to examine what is working for custodians, their staff and their patients. For example, do patients have the digital health literacy required to use (or continue to use) some of the new tools developed? Do you or your staff require any additional training, do any policies and procedures need to be reviewed or developed?

If you have not already, it is best practice to review your current tools to ensure they reflect new ways of doing things. For example, if appointments are being offered virtually or by phone on a more permanent basis, a privacy notice posted in the clinic waiting room will not be as effective as it was when appointments were in-person.

Some changes you have experienced in 2020 may be short term; however, many may become permanent. Custodians should examine what is effectively working for themselves, their staff, and their patients. Regardless, it is imperative that *PHIA* compliance remain a consideration. The OIPC has developed a number of *PHIA* resources for custodians, available on our website at <https://www.oipc.nl.ca/custodians>. Some specific guidance pieces that may be of assistance include:

- [PHIA compliance checklist](#) - even if you have completed this checklist before, if you have adopted new technology or experienced other changes in processes, it is best practice to revisit the checklist to ensure that your changes have not impacted *PHIA* compliance.
- Use of E-mail - OIPC has developed two guidance pieces on the use of e-mail, including a [quick tips](#) document and a more detailed [document](#) with considerations if personal health information is being sent by email.

Review of Recent Decisions and Reports

[Saskatchewan Health Authority \(Re\), 2020 CanLII 84508 \(SK IPC\)](#)

In April 2019, it was discovered that a physician at Rosetown Primary Care Centre (RPCC) in Rosetown, Saskatchewan had been inappropriately accessing the electronic medical records of Town employees and other individuals who were not his patients.

During an investigation into the matter, the Saskatchewan Health Authority (SHA) determined that the electronic medical files of at least 20 individuals had been accessed inappropriately.

The SHA notified the affected individuals that their medical records had been accessed, but did not explain by whom – only that the person was not involved in their medical care. The RPCC employed both physicians, who were contracted by SHA, and staff, who were employed by the Town. The lack of specificity as to who accessed the records caused confusion and anger amongst those affected.

One individual made a complaint to the Saskatchewan Information and Privacy Commissioner, stating that there was a lack of accountability, as the physician did not admit to any wrongdoing, offered no apology, and was not disciplined (due to being a contractor and not an SHA employee).

Among the several issues addressed in the Report, the Commissioner reaffirmed that physicians “do not have a static entitlement to patients’ personal health information” and that each access should be made only when there is a need-to-know basis.

The Commissioner also noted that affected individuals deserve to know all the details regarding inappropriate accesses to their personal health information:

My office’s position is that an individual who has snooped should have a diminished expectation of privacy. Their identities and the disciplinary action taken against them should be revealed to affected individuals. The impact of a privacy breach is not standard and flat. Learning that a best friend, business partner, estranged spouse, co-worker, boss, neighbour, or a stranger snooped upon one’s personal health information has different implications for individuals. Affected individuals are in the best position to understand the impacts of a privacy breach upon themselves. Knowing the identity of the snooper provides affected individuals with information to assess the harm that may result from having their privacy invaded. In my Investigation Report 100-2015, I cited the former Ontario Information and Privacy Commissioner’s Investigation Report HO-010 that provided that aggrieved individuals have a right to a complete accounting of what has occurred. Aggrieved individuals will not find closure regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that “the incident has been dealt with appropriately” falls far short of the level of disclosure that is required. Further, publicly identifying the snooper and the disciplinary action taken against the snooper would be a strong deterrent for other employees and contractors.

The Commissioner subsequently recommended that SHA send another letter to affected individuals, properly advising them of the situation, including the identity of the physician, actions taken against him, and actions SHA have taken to mitigate future breaches.

[Service Coordination Support \(Re\), 2020 CanLII 85021 \(ON IPC\)](#)

Service Coordination Support (SCS) in Ontario received an access to information request from an applicant seeking records relating to her son under the *Personal Health Information Protection Act (PHIPA)*. Although the original complaint concerned the quality of the search for records, the Adjudicator realized that the SCS might not be a “health information custodian” within the meaning of the Act.

The Adjudicator reviewed the definition of “health information custodian” within *PHIPA*, considering whether SCS was “a centre or program or service for community health or mental health whose primary purpose is the provision of ‘health care.’”

Briefly, the SCS is a service agency assisting adults and children with developmental disabilities or autism spectrum disorder. Among its services, it provides support for parents of children with disabilities, including matching families with respite workers; provides opportunities, resources, and supports to adults with disabilities; coordinated service planning for young people; and other community services.

The Adjudicator noted that, even though the program participants may have health challenges and also that some third party entities might be health information custodians, this does not mean that the SCS itself is one:

[34] In my view, what is common to each of the six services offered by SCS is SCS' role as a coordinator for, or link to, a wide range of services offered by third parties to individuals with developmental disabilities and/or autism. It is a role of coordination between these individuals (or their family members) and third-party services, which may include assessing each individual's needs and/or preferences, and matching them to various types of programs in the community. The effect of the individuals' participation in those third-party programs may well be that it enhances their health, but that does not transform SCS' role into one that can be described as having a primary purpose of providing health care. In my view, it would be too broad a reading of "health care" to find that SCS' primary purpose is the provision of health care.

As a result, the complaint was dismissed.

Complaints and Breach Notifications

Between September 1, 2020 and November 25, 2020, the OIPC received the following breach notifications and complaints related to *PHIA*:

- 12 breach notifications were sent to this Office following an incident. The majority of these breaches occurred within the regional health authorities.
- The OIPC received two complaints related to *PHIA* during the same period of time.

Per section 15(4) of *PHIA*, material breaches – inappropriate collection, use, or disclosure of personal health information – must be reported to the Commissioner via the breach reporting form from the OIPC.

Despite the COVID-19 Pandemic, compared with statistics from the same period of time in 2019, *PHIA* complaints to the OIPC are substantially fewer (11 in 2019); however, breaches have increased (4 in 2019).