SAFEGUARD

A QUARTERLY NEWSLETTER PUBLISHED BY THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

VOLUME 2, ISSUE 3 OCTOBER 2018

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
Tel: (709) 729-6309
Fax: (709) 729-6500
Toll Free in Newfoundland and Labrador: 1-877-729-6309
E-mail: commissioner@oipc.nl.ca
www.oipc.nl.ca

"Thus, at least in part, medical records contain information about the patient revealed by the patient, and information that is acquired and recorded on behalf of the patient. Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that goes to the personal integrity and autonomy of the patient."

- Justice La Forest
McInerney v. MacDonald, [1992] 2 SCR 138 (SCC)

OIPC REMINDERS AND UPDATES

THE OIPC NOW HAS A BLOG

The OIPC has launched a blog. The blog will provide an opportunity for our staff to comment on topics of interest and discuss developments in access and privacy. The entries are the personal comments of staff, do not constitute legal advice and cannot be relied on as such. Any comments or opinions expressed in the blog posts are not binding on the Information and Privacy Commissioner of Newfoundland and Labrador.

BUILDING IN AND REVISITING PRIVACY

As custodians move forward in creating their Privacy Management Programs, they are reminded that while it is important to ensure that privacy is built into all new programs or services of a custodian, the legislative obligations are equally applicable to programs and services already in existence. Custodians should revisit and reexamine the privacy implications of standing programs and services to ensure that they are in line with *PHIA*.

THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA RESOURCES

The Office of the Privacy Commissioner of Canada has developed a series of privacy cartoons that are available for printing and posting.

Practice Tip — Contact Professional and Regulatory Bodies

Custodians who are members of regulated professions or professional associations should reach out to those organizations to determine if they offer *PHIA* training or template materials. These tools are useful for all custodians but may be particularly helpful to custodians in sole practice or small clinics.

THE USE OF APPS BY CUSTODIANS

Increasingly, custodians are using software applications ("apps") in an attempt to streamline processes and provide citizens with an alternative method to interact with custodians.

Custodians must be aware that their legislative responsibilities in relation to personal information continue even if the app is created and maintained by an outside vendor. When contemplating whether to use or offer apps, public bodies should consider the following:

What is the Nature of the App?

Will the app be required, recommended, endorsed or simply suggested as an option by the custodian?

Offering an app allows individuals to make a choice about whether they want to consent to the use of their personal information by the app.

Requiring, recommending or endorsing the use of an app places a greater obligation on a custodian to review the vendor's privacy statement, terms of use and permissions and to ensure that the vendor's collection, use and disclosure of users' personal information is in accordance with the *PHIA.*

What Need will the App Address?

Custodians must consider whether the use of an app is the most appropriate way to address the specific identified need/gap.

How will Information be Provided to the App?

Will the custodian be pushing personal information to the app or will individuals provide the information themselves?

Will the Custodian Pull Information from the App?

If custodians intend to pull information from an app, this is an indirect collection and custodians must make certain to put agreements in place that ensure *PHIA* compliance.

Privacy Statements, Terms of Use, Permissions

Custodians must review the privacy statements of all apps being required, recommended or offered.

Where an app is required, custodians must ensure that there are no provisions within the privacy statement that are contrary to the obligations set out in the *PHIA* and this process should be documented, preferably through a PIA.

In all instances, the privacy statement of the app must be available to the public. Custodians should consider encouraging individuals to review the privacy statement and may, in some instances, determine that a summary of key points should be developed.

We will be issuing a detailed guidance document on this topic in the near future.

PRACTICE TIP

A request for access to personal health information can be made by a representative of the individual who the information is about. These representatives can take a number of appearances, as outlined in section 7 of *PHIA.* Custodians should develop an internal policy and authorization form to be used in relation to those representatives acting under written authorization.

INTERESTING DECISIONS FROM OTHER JURISDICTIONS

Office of the Information and Privacy Commissioner for Nova Scotia - Investigation Report IR18-01

Following a prompt from the Nova Scotia College of Pharmacists, the Department of Health and Wellness conducted an audit of user activity. The prompt arose out of concerns which were raised in relation to a registered pharmacist's use of the provincial Drug Information System (DIS). Following the audit, the Department, along with Sobeys National Pharmacy Group ("Sobeys"), conducted an investigation into the actions of the pharmacist who was employed by Sobeys as a manager at a rural pharmacy. The investigation determined that the pharmacist had inappropriately accessed the personal health information of 46 individuals. The pharmacist was subsequently terminated from employment with Sobeys.

The OIPC NS conducted its own investigation of the matter once it was notified of the situation by the Department. This investigation revealed that the inappropriate accesses occurred over a 2-year period and included accesses to the personal health information of the pharmacist's doctor, co-workers, former classmates, her child's girlfriend and her parents as well as teachers in her child's school among others. The OIPC also determined that in order to gain access to certain personal health information, the pharmacist created false profiles in the DIS and falsely claimed that she had the individuals' consent to create records. There was also evidence that the pharmacist used and disclosed the personal health information which she accessed even after her employment was terminated.

In addition to making determinations regarding the actions of the pharmacist, the investigation by the OIPC NS also highlighted the failings of the initial investigation conducted by the Department and Sobeys including the insufficient canvassing of the risks and, as a result, the insufficient containment of the breaches. This Report relates to the Department. A second companion Investigation Report (IR18-02) relates to Sobeys.

OIPC NS identified a "critical vulnerability" in governance and monitoring of broad access, multi-custodian, electronic personal health information databases and stressed the urgent need to strengthen and clarify the responsibilities for and monitoring of interoperable health information databases.

The OIPC NS found that:

- the Department does not have an adequate or effective breach investigation protocol;
- the Department failed to identify and properly notify all affected individuals;
- any effective administrative safeguards which were in place are insufficient to protect against snooping and were not effectively used;
- the Department was not adequately auditing organizations that have been granted access to the DIS; and
- the Department does not have sufficient safeguards in place to protect its electronic health information systems.

(Continued on next page)

INTERESTING DECISIONS FROM OTHER JURISDICTIONS

Consequently the OIPC NS recommended:

1. The Department develop and implement an effective investigation protocol for the DIS that ensures the Department takes the lead and has authority to determine corrective action.
2. The Department re-contact all 46 affected individuals to determine if the pharmacist has been in contact with them since April 2018. If so, the Department must take further legal action to prevent the ongoing unauthorized use or disclosure of the personal health information.
3. The Department revise its Privacy Breach Protocol to prescribe that where a user is found to have breached the privacy of any individual(s) via one of the electronic databases, detailed audits of that user's activity in other implicated databases are automatically conducted.
4. The Department revise its Privacy Breach Protocol to clarify that notification at the first reasonable opportunity requires that notification occur within days and to ensure that notification letters include clear and specific information regarding the breach.
5. The Department establish a protocol for investigating anonymous tips on its Health Privacy 1-800 line.
6. The Department amend the DIS User Agreement to make it mandatory that user organizations monitor and audit their own systems and to make the type and frequency of the Department monitoring of user organization audits and audit capacity explicit.
7. The Department conduct training for all users of the DIS on the use of DIS notations to ensure any use of the DIS not associated with prescription activity is explained.
8. The Department update its Privacy Policy to reflect current positions and to remove ambiguity about agency status of individuals not employed by the Department.
9. The Department develop more robust and systematic auditing policies and practices.
10. The Department amend *PHIA* to add provisions that assign responsibilities for interoperable health databases in use in Nova Scotia to prescribed entities.

Office of the Information and Privacy Commissioner for Nova Scotia - Investigation Report IR18-02

This is the companion Investigation Report to IR18-01, outlined above. The background and factual information are the same.

In this Report, the OIPC NS found:

- Sobeys failed to act in a timely fashion to properly and thoroughly investigate and contain these privacy breaches;
- false profiles continue to exist on the system and, as a result, the breach has still not yet been adequately contained; and
- Sobeys has several effective administrative safeguards in place and took effective steps to remediate the work environment following these breaches; however, Sobeys does not have adequate technical auditing capacity to detect unauthorized access by authorized users.

(Continued on next page)

INTERESTING DECISIONS FROM OTHER JURISDICTIONS

The OIPC NS recommended:

1. Sobeys develop and implement a privacy breach management protocol and provide training on the protocol to management within six months.
2. Sobeys immediately notify the 28 individuals whose personal information was improperly copied into its POS system.
3. Sobeys delete all false profiles from the POS system after providing a copy of the record to affected individuals.
4. Sobeys update, within 45 days, its Operational Standards for pharmacies in Nova Scotia and information brochures intended for Nova Scotian customers to include a correct reference to Nova Scotia's *Personal Health Information Act* and the privacy complaints process.
5. Sobeys make documenting the reason for DIS access for non-dispensing situations mandatory for all pharmacy staff.
6. Sobeys require all pharmacy staff to read this report.
7. Sobeys improve its Quality Improvement Audit process by doing it more frequently, involving more management and non-management staff and including a regular review of the audit logs for the POS system.
8. Sobeys obtain and implement the technical auditing capacity to regularly conduct proactive user activity audits of its POS system within six months.

Office of the Saskatchewan Information and Privacy Commissioner IR 024-2018

In our February 2018 newsletter we reported on an investigation by the College of Physicians and Surgeons of Saskatchewan into the actions of a Regina doctor who altered the medical records of a deceased individual. The physician admitted guilt in that matter. This is the decision of the Saskatchewan Commissioner in relation to the matter.

The Commissioner found that the physician did not have proper policies and procedures in place and was not in compliance with the *Health Information Protection Act*. The Commissioner's recommendations included having the physician research best practices with respect to the timeliness of completing notes, making corrections to personal health information, adding late entries to personal health information and blocking access to personal health information. The Commissioner further recommended that the physician create a privacy impact assessment and policies and procedures. The physician was identified both by the College and the Commissioner.

Did you know you can follow our Office and other IPC Offices across the country on Twitter for discussions on interesting access and privacy developments?

Check us out at @OIPCNL

HACKING FAX MACHINES

Antiquated fax protocols may be opening the door for cyber attacks. At the recent Def Con hacker conference in Las Vegas, research was presented indicating that holes in fax protocols – which define the format of fax messages – allow hackers to enter corporate networks.

Many fax machines currently double as printers and photocopiers and, as a result, have a network connection, usually to an internal network. Once the hackers have access to the internal network, they can attack the user on a larger scale.

Although many manufacturers were affected, HPs multi-purpose printers were highlighted based on their widespread use. HP has indicated that it has issued a patch for the issue.

RECENT OIPC REPORT

Report AH-2018-001 — Eastern Health

An Applicant, acting as a substitute decision-maker, requested notes and other information in relation to his parent. Eastern Health responded to the Applicant's request, providing 57 pages of records. These records were subject to numerous redactions to remove the names and other identifying information of third party individuals interviewed and consulted in the process of conducting an investigation under the *Adult Protection Act* ("APA"). The Applicant believed he was entitled to the entire record.

The Commissioner explained that a custodian is required by section 58(1)(d)(ii) to withhold information that could reasonably be expected to lead to the identification of persons compelled to provide information and the *APA* compels individuals to cooperate with an investigation under that *Act*. The "identifying" information in this case were personal pronouns that would identify a person's sex and references to the individual's relationship to the Complainant's parent. The Commissioner found that it is reasonable to assume that any investigation into the welfare and well-being of an individual will include the family members of that individual and members of the community close to them. The Commissioner further found that this may be a small group who may be easily identified with such terms as "his mother", "her father", etc. Accordingly, any terms disclosing the sex of an individual or their relation to the subject of the investigation could reasonably be expected to lead to the identification of that person. The Commissioner held that Eastern Health was correct in refusing to release the information and the Complainant, as the substitute decision maker for his parent, had been provided with all of the information to which he was entitled in order to make health care decisions for his parent. The Commissioner concluded that that the right or power of a substitute decision maker to exercise an individual's right to access their personal health is still subject to the restrictions articulated at section 58 of the *PHIA*.

HEALTHe NL CONTINUES TO GROW*

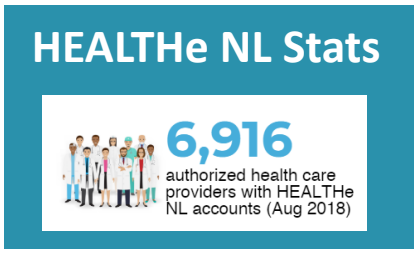
Newfoundland & Labrador Centre for Health Information

The Centre is responsible for developing and implementing the province's confidential and secure electronic health record called *HEALTHe NL*.

HEALTHe NL is a private record of an individual's health care information, available electronically to authorized health care professionals. It integrates information from many sources into a single, lifetime record of an individual's key health history and care. Information is available in one place when and where it is needed.

HEALTHe NL currently includes the following types of information, which is updated daily, and helps support real-time health care decision-making at the point of care.

- Patient medication profiles from all provincial community pharmacies.
- Known allergies and medical alerts collected by community pharmacies.
- Provincial immunization data for anyone born after 2003.
- Regional Health Authority Meditech data, including dictated reports, laboratory results, diagnostic imaging and encounters. The remaining data to complete the EHR build is the integration of Central Health's dictated reports and diagnostic imaging and is expected be added this summer.
- Information about where health services have occurred, by whom and other key clinical events such as inpatient admission.
- Additional data and functionality continue to be assessed and added.



The key to all of NLCHI's work is that it is provincial in scope – it's available to all clinicians in the Province, regardless of their location. The opportunities to improve patient safety and quality of care, and create work flow efficiencies are boundless.

Learn more about *HEALTHe NL* or sign up to be a *HEALTHe NL* user!

service@nlchi.nl.ca or 1-877-752-6006 or

https://www.nlchi.nl.ca/index.php/ehealth-systems/healthe-nl.

*Written by and reproduced with the permission of the Newfoundland and Labrador Centre for Health Information.

PHIA COMPLIANCE CHECKLIST

This Fall the OIPC will be issuing a *PHIA* Compliance Checklist. This document will be circulated to the professional, governing and regulatory organizations of custodians for distribution to their membership. Our objective with this initiative is to help Custodians ensure they are meeting their obligations under *PHIA.*

Please keep an eye out for your copy of this useful tool.