SAFEGUARD

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

Volume 8, Issue 3 August 2024

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

Website:
www.oipc.nl.ca

Follow us on social media!

LinkedIn:
https://Linkedin.com/company/oipc-nl

This Issue:

Personal Health Record – Update!

Earlier this year, our February issue of Safeguard announced that the Provincial Government and Newfoundland and Labrador Health Services (NL Health Services) was introducing a new online service to improve access to the health care system.

Individuals would be able to access some of their health information online through MyGovNL. The online service was to be initially available to a small number of individuals and then increasing the number of individuals with access over time.

The Personal Health Record gives you access to your laboratory results, dispensed medications, allergy information, and x-ray reports.

This service is now widely available and individuals can register for the Personal Health Record on MyGovNL to access their health information.

For enhanced security, registrants will receive a personal identification number via regular mail within two weeks to complete the registration process. This activation code is required for the first time you log in to your personal health record. You will also need to have a government issued photo identification card and your MCP connected through MyGovNL as well as an email address.

To register for the personal health record:

- log in to MyGovNL;
- click Personal Health Information;
- submit the registration form; and
- enter the personal identification number when you receive it in the mail.

Custodians and Health Research

Health research involving human subjects must be approved by the Health Research Ethics Authority as required by the **Health Research Ethics Authority Act** (HREAA). This approval is based on the statutory requirements of HREAA that focus on ethics.

While privacy considerations come into play in an ethics review, custodians cannot rely on the Research Ethics Board's approval to satisfy their PHIA obligations to protect personal health information. When a custodian shares information as part of an approved research project, the custodian should clearly establish expectations regarding retention, destruction and future use of data. Custodians must also ensure that they are aware of the safeguards in place to protect the data, which could include administrative safeguards, such as agreements that require prompt notification if the information is compromised, such as in a breach or security incident situation.

Security threats to research data are predictable and the Canadian Centre for Cyber Security even offers courses for researchers, e.g. Cyber Security for Researchers and Introduction to Research Security. Custodians should consider if a security assessment is required for tools used to collect, store and protect personal health information during the research process.

OIPC has developed guidance titled Disclosure of Personal Health Information for Research Purposes: Guidance for Researchers and Custodians of Personal Health Information to assist health custodians and researchers.

OIPC has also developed a Compliance Checklist that may assist custodians. While not specific to health research, it does contain high level details of obligations under PHIA, such as ensuring the appropriate safeguards are in place.

Custodians are reminded that privacy legislation is not a barrier to health research and that PHIA better ensures that personal health information is protected during research initiatives.

Reasonable Safeguards

Custodians must have reasonable safeguards in place, as section 15 of PHIA establishes security expectations, stating, in part:

> 15. (1) A custodian shall take steps that are reasonable in the circumstances to ensure that
>
> (a) personal health information in its custody or control is protected against theft, loss and unauthorized access, use or disclosure;
>
> (b) records containing personal health information in its custody or control are protected against unauthorized copying or modification; and
>
> (c) records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner.

How does section 15 of PHIA apply when using a third party vendor?

Custodians are reminded that they cannot "contract out" of PHIA as it is a law, however they can use contracts as an administrative safeguard.

If custodians are using a third party vendor for information processing, handling, or storage, they should ensure that there are contractual and oversight measures in place to ensure the privacy and security of personal health information (PHI) in accordance with the requirements of the legislation and its regulations.

The following are some considerations when entering into a contractual agreement with a third party vendor. Does your contractual agreement:

- Confirm your continued custodianship and control of the data, or PHI provided;
- Require the third party vendor to demonstrate that their personal information data handling capabilities are in compliance with legislative requirements;
- Obligate the third party vendor to promptly notify you of any incident or breach involving PHI that you provided;
- Include any specific contract provisions that limit the collection, use and disclosure of PHI to authorized purposes and by authorized staff;
- Provide for the confidentiality and security of PHI (e.g. secure storage and transmission, encryption, authentication for access);
- Allow for any subcontracting of services involving the handling of PHI you have entrusted with the third party vendor? If so, what provisions are in place to ensure compliance with applicable legislation;
- Establish a process for dealing with the compelled disclosure of PHI to third parties (e.g. courts, law enforcement);
- Require or allow audits of the third party's practice and procedures to ensure privacy and security compliance;
- Include provisions regarding the training of staff and management on legislative requirements for Newfoundland and Labrador clients;
- Return or secure disposal of PHI by the vendor upon termination of the agreement; and
- Include measures for implementing, administering and enforcing the agreement between the custodian and the vendor.

A custodian should consider what information the third party vendor will provide if there is an incident or a breach. For example, will the third party vendor provide the custodian with the following details:

- what happened;
- when was the issue discovered;
- how was the issue discovered;
- what steps have been taken to contain the breach;
- what steps still need to be taken;

- what electronic information was affected;
- how long was the information affected/unprotected; and
- how many individuals were affected (overall, as well as for the information provided by the custodian)?

Custodians with questions on the above, or on other PHIA compliance topics, can refer to the resources under the Custodians tab on our website, as well as from the Department of Health and Community Services.

Breach Notification Reminders

Section 15 of PHIA discusses breaches and the custodian's duty to notify impacted individuals.

When a breach impacts a large number of individuals, it is not uncommon for the OIPC to receive a large volume of calls. Some of the most common calls our Office receives when there is a breach are:

- callers seeking specific information about the breach and how it relates to their information;
- callers expressing frustration that they have been unable to reach anyone at the number provided in the custodian's notification letter;
- callers requiring assistance with credit monitoring services; and
- callers seeking reassurance that the notification letter about the breach is not a scam.

If the custodian has notified OIPC about the breach then our Office can confirm with callers that the notification letter is not a scam and advise callers that we are aware of the breach. However, our Office would not be able to advise individuals on their specific information that was breached nor are we able to provide assistance with credit monitoring.

Based on this experience, in addition to legislative requirements for breach letters, we recommend the following best practices.

- Be clear who can be contacted at the organization where the breach occurred and ensure there are appropriate resources to respond to the anticipated volume of calls. Make this **contact information** the most **prominent** on the notification letter so individuals can easily see what number to call.
- If a third party provider has been contracted to assist in breach management, such as a call center, make this clear.
- If there are multiple contact numbers, consider including details on which contact to use for which purposes. For example, provide a specific number for help with setting-up credit monitoring.
- Advise individuals if they wish to make a complaint they must contact OIPC, however, **do not** make our Office's contact information the most prominent on the notification letter as individuals may be confused thinking that our Office can provide specific details about the breach.

New Forms and Guidelines - Reminder!

In our last issue of Safeguard we announced that we had launched a new website and also had new forms and guidelines!

We wanted to remind custodians about the new guidelines and we hope they will provide assistance when custodians respond to access, correction or privacy complaints. Please review these guidelines on our Complaint Process webpage for Custodians.

We also wanted to remind complainants that we have new complaint forms for complainants to use. Please visit our Public Forms webpage to view these forms.

Upcoming Events – Save the Date!

Right to Know Week – September 23 - 29, 2024

Right to Know Day is on September 28th every year. It is an internationally recognized day dedicated to creating awareness about the importance of people's right to access government information, while promoting freedom of information as essential to both democracy and good governance.

Right to Know Day now extends to a week of celebrations, known as Right to Know Week, which will take place this year from September 23 - 29, 2024.

Join our Office along with other provinces and territories across Canada in celebrating Right to Know Week!

Please check our website or contact our Office for updates on activities and plans in celebrating Right to Know Week!

APSIM Conference – November 28 - 29, 2024

The Access, Privacy, Security and Information Management (APSIM) Conference is scheduled for November 28th and 29th this fall. This will be an in-person conference in St. John's, NL. There will also be a virtual half-day municipal specific workshop, which will take place a few days prior to the conference (date to be confirmed).

This conference aims to bring together members of the Newfoundland and Labrador access, privacy, information security, and information management communities to promote collaboration and build awareness of the overlap and interplay between these various disciplines.

This conference is intended for individuals working within the public sector, health care community, and anyone interested in access, privacy, security, and information management issues.

Please check our website or contact our Office for updates on APSIM and registration deadlines!

PHIA Privacy Breach Statistics May 1, 2024 – July 31, 2024

Between May 1, 2024 and July 31, 2024, breach notifications continued to increase with OIPC receiving 16 breach notifications. The 16 breach reports came from seven different custodians. Some of the breaches involved personal health information being sent to the wrong individual either by mail or email. Of note, there were a couple of cybersecurity breaches involving unauthorized access to information systems. The custodians involved have investigated the incidents to determine the extent of the breach and indicated that they have contained the breaches.

Want Training?

We would like to remind custodians that OIPC offers PHIA training that can be customized to their needs!

Interested custodians should email OIPC at commissioner@oipc.nl.ca.

There are also a number of PHIA resources available on OIPC's website.