



# SAFEGUARD

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

Volume 10, Issue 2

May 2026

## Contact Information

Office of the Information and Privacy Commissioner

Mailing Address:  
PO Box 13004, Station A  
St. John's, NL A1B 3V8

Telephone:

709-729-6309

Toll Free in Newfoundland and Labrador:

1-877-729-6309

Email:

[commissioner@oipc.nl.ca](mailto:commissioner@oipc.nl.ca)

Website:

[www.oipc.nl.ca](http://www.oipc.nl.ca)

Follow us on social media!

LinkedIn:

<https://LinkedIn.com/company/oipc-nl>

## This Issue:

- Updates
- Privacy in Practice: Use of Email to Communicate with Clients
- Substitute Decision Maker: Spotlight on Section 7(b) and Access Requests
- PHIA Privacy Breach Statistics February 1<sup>st</sup> – April 30<sup>th</sup>

## Updates

### APSIM Conference

The APSIM Conference, scheduled for November 26 and 27, 2026, continues to welcome speaker proposals. This two-day in-person event will again take place at the Health Innovation Acceleration Centre in St. John's, and will bring together access, privacy, security, and information management professionals. For the latest updates and information about APSIM, please visit the Conference's [official website](#). If you have questions, please contact [APSIMconference@gov.nl.ca](mailto:APSIMconference@gov.nl.ca).

### Social Media

OIPC is expanding our social media presence! OIPC NL Instagram and YouTube accounts will soon be active, along with a new social media policy.

### Feedback

If you have any questions or feedback about our forms, guidelines or guidance, including suggestions on topics for guidance resources, please let us know!

## Privacy in Practice: Use of Email to Communicate with Clients

This is a new column, created in response to feedback gathered during OIPC's recent survey on our guidance, newsletter and conference. This column will present a scenario and identify PHIA considerations; it is hoped that this will help custodians in their everyday work. If you have a scenario you would like to see featured, let us know by emailing [commissioner@oipc.nl.ca](mailto:commissioner@oipc.nl.ca) with the subject "PHIA Scenarios."

**Scenario: I am a custodian considering using an email account to communicate with clients. What should I consider?**

Both custodians and clients may find communicating using email convenient and efficient. But what does PHIA say?

Personal health information is defined in section 5 of PHIA. Email communication would include, at minimum, the client's email address, name, the purpose for the email (such as an appointment request), and possibly alternate contact information, such as a phone number. This registration information would all be considered personal health information as defined by PHIA and collected by the custodian for the provision of health care. It is possible that email communication could involve much more sensitive or detailed health information as well.

No matter how custodians communicate with clients, they need to ensure that reasonable safeguards are in place. In order to determine what safeguards are reasonable, one must understand all of the relevant considerations. For example:

- What email address will be used?
  - Does the custodian use the same email address for other things, like personal matters, or have they created an email that will exclusively be used for client communication?
  - It is considered best practice to have an email dedicated exclusively to their work as custodian.
- Who has access to the email?
  - Is the email accessible to others, such as employees or contractors (i.e. a receptionist)?
  - If using a personal device, is it accessible by others, such as a partner or family member, and is it backed up to a cloud owned by a linked account, such as a family cloud?
  - Best practice would be to ensure that the only people who should have access to the email account are those that need access for a valid reason in accordance with PHIA.
- What information will be communicated using email?
  - For example, will clients be able to request appointments and maybe receive appointment reminders, or will more sensitive personal health information be communicated, such as MCP, date of birth or test results?
  - If sending reminders, ensure the minimum information necessary is included, such as a time and date and no details of the reason for the appointment.

Once the custodian has a better understanding of their own email practices or plans, they should consider appropriate safeguards, including the following:

- Ensuring that only the minimum necessary personal health information is collected, used and disclosed. Custodians could consider a caution that encourages patients to limit information provided and identifies what should be included in any correspondence. This could be done on any website that features their email address, as well as placing a note in their email signature about what information should be included in any correspondence.
- Depending on the sensitivity of the information being communicated, custodians may want to consider including best practices for clients. For example, recommending they use a personal email and not a work account.
- Clarifying the custodian's relationship with their email provider; are they an agent, an information manager, or something else?
- Reviewing the contract with their email provider and, if there is no contract, their privacy policy, as well as terms and conditions of use.
- Enabling appropriate security features. For example, email providers offer things like confidential modes, encryption, and two-factor authentication.
- Determining any changes required for their information handling practices. For example, will custodians transfer information from the email to their electronic system and if so, the steps they will take to ensure its accuracy and that only the minimum necessary information is transferred. As well, custodians should review their breach process to ensure that they have a plan to contain and manage breaches that occur because of mis-directed emails.
- Ensuring that emails are deleted in a timely fashion.
- Reviewing their privacy notice to identify any modifications that may be required to reflect the use of email, including how it will be used (for example, appointment reminders, etc.)
- Ensuring proper policies are in place regarding granting or revoking access to third parties such as receptionists, trainees, etc.

Custodians are reminded that any communication with clients requires reasonable safeguards. Taking proactive measures can avoid issues down the road.

## Substitute Decision Maker: Spotlight on Section 7(b) and Access Requests

Section 7(b) of PHIA states that a right or power of an individual under PHIA may be exercised:

Where the individual lacks the competency to exercise the right or power or is unable to communicate, and where the collection, use or disclosure of his or her personal health information is necessary for or ancillary to a "health care decision",

as defined in the Advance Health Care Directives Act, by a substitute decision maker appointed by the individual in accordance with that Act or, where a substitute decision maker has not been appointed, a substitute decision maker determined in accordance with section 10 of that Act;

The [Advance Health Care Directives Act](#) (AHCDA) defines “health care decision” and “substitute decision maker” in section 2:

- (b) "health care decision" means a consent, refusal to consent, or withdrawal of consent of any care, treatment, service, medication, or procedure to maintain, diagnose, treat, or provide for an individual's physical or mental health or personal care and includes
  - (i) life-prolonging treatment,
  - (ii) psychiatric treatment for a person other than a person admitted to a psychiatric unit as an involuntary patient under section 24 or detained in a psychiatric unit under subsection 81(4) or released into the community under a community treatment order under subsection 40(2) of the Mental Health Care and Treatment Act,
  - (iii) the administration of nutrition and hydration, and
  - (iv) admission to treatment facilities and removal from those institutions, other than the admission, transfer, removal or discharge of a person admitted as an involuntary patient under section 24 or detained in a psychiatric unit under subsection 81(3) or released into the community under an assisted community treatment order under subsection 40(2) of the Mental Health Care and Treatment Act;
- ...
- (e) "substitute decision maker" means the person appointed by the maker of an advance health care directive to make health care decisions on his or her behalf.

But what happens to the rights of the substitute decision maker as a representative when the individual is deceased? Section 52(1) of PHIA establishes an individual's right of access to a record containing his or her personal health information that is in the custody or under the control of a custodian. This right of access can be exercised by representatives of an individual, including representatives of deceased individuals. However, access to information after the individual is deceased does not fall under the definition of health care decisions that the substitute decision maker is authorized to make. As such, an individual who was a substitute decision maker is not entitled to information about the deceased individual unless they are also considered a representative under another subsection of Section 7. For example, they may be a personal representative as contemplated in section 7(e).

## PHIA Privacy Breach Statistics February 1<sup>st</sup> – April 30<sup>th</sup>

Between February 1 and April 30, 2026, OIPC received five privacy breach notifications, which is a decrease over last quarter's 10 breaches. The five breach reports came from three different custodians. Two breaches involved issues with mailouts, one with technical issues with a system, and two were intentional.

Custodians are reminded that OIPC will only be accepting privacy breach reports that are sent using the official OIPC [Privacy Breach Reporting Form](#). All other reporting forms will be rejected, and the custodian will need to re-submit. Additionally, custodians are reminded that personal health information should not be included in the breach reports submitted to this Office.

As well, please ensure your breach notification letters to impacted individuals reflect our new physical address: 5th Floor, Beothuck Building, 20 Crosbie Place, St. John's NL. Our mailing address remains the same: PO Box 13004, Station A, St. John's, NL, A1B 3V8.

### Want Training?

We would like to remind custodians that OIPC offers PHIA training that can be customized to their needs. We are available to speak at annual general meetings and other events on a variety of access and privacy topics pertinent to custodians.



Interested custodians should email OIPC at [commissioner@oipc.nl.ca](mailto:commissioner@oipc.nl.ca).

There are also a number of PHIA resources available on OIPC's [website](#).