SAFEGUARD

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

Volume 7, Issue 4 November 2023

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!

Twitter:
@oipcnl

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

This Issue:

- NEW Guidance – *PHIA* Toolkit for Small Custodians (Summary Part 2)
- Podcast Discussion on OIPC Cyber Attack Report
- Increasing Access to Health Care Through Virtual Care Contract
- Searching for Personal Health Information
- Reminder – Use of Email for Communicating Personal Health Information
- Breach Notifications

NEW Guidance – *PHIA* Toolkit for Small Custodians (Summary Part 2)

Our Office released new guidance for small custodians – *PHIA* Toolkit for Small Custodians on March 31, 2023. As this guidance piece is detailed, we have broken it down into two parts. We covered the definitions of custodian, agent and information manager as well as some custodian obligations under *PHIA* in Summary Part 1 in Safeguard - Volume 7, Issue 2, May 2023.

In this issue, Summary Part 2 will cover security as it relates to personal health information; collection, use and disclosure of personal health information; and access and correction of personal health information. A review of the full guidance piece is still recommended and can be found on our website.

A reminder from Summary Part 1:

- *PHIA* applies to custodians who have custody or control of personal health information as a result of or in connection with the performance of their powers, duties or work. *PHIA* outlines obligations for all custodians, regardless of the size of their organization.

- This toolkit is intended as a guide to help small custodians, such as individual health care professionals/practitioners and private long term care facilities, understand and comply with their obligations under *PHIA*.

Security

Custodians must ensure they are adequately protecting an individual's personal health information at all times. A custodian must take reasonable steps to ensure that personal health information in its custody or control is protected against theft, loss, unauthorized access, use, disclosure, copying or modification and that it is retained, transferred and disposed of in a secure manner.

There are different ways a custodian can protect personal health information and knowing what personal health information is involved will help determine what measures to use to protect it. Some examples of safeguards are:

- Administrative Policies – using administrative polices include written policies outlining the custodian's instructions in respect of collecting, using and disclosing personal health information and the rules to effectively safeguard personal health information.

- Technical Safeguards - using technical safeguards could include implementing access controls restricting the personal health information that employees can access. Access controls can help limit snooping and other unauthorized access to personal health information.

- Physical Safeguards – using physical safeguards include locking doors, filing cabinets, and rooms with restricted access. A monitored alarm system or using electronic access cards for gaining access to the premise are also examples of physical safeguards.

Collection, Use and Disclosure of Personal Health Information

The definitions for collect, use and disclose are found in section 2 of *PHIA* and are as follows:

> "Collect" means to gather, acquire, receive or obtain the information by any means from any source and "collection" has a corresponding meaning.
>
> "Disclose" means to make the personal health information in the custody or control of a custodian or other person available or release it but does not include a use of the information and "disclosure" has a corresponding meaning.
>
> "Use" means to handle or deal with the personal health information in the custody or control of a custodian or to apply the information for a purpose and includes reproducing the information but does not include disclosing the information.

A custodian shall not collect personal health information about an individual unless:

- the individual who is the subject of the information has consented to its collection and the collection is necessary for lawful purposes; or

- the collection is permitted or required by *PHIA*.

A custodian must not collect more personal health information than is reasonably necessary to meet the purpose of the collection (section 32). Think of it as a "need to know" principle and a good practice is to ask "Am I collecting too much information?" If you don't need the information then don't collect it.

Collections, uses and disclosures of personal health information under *PHIA* are, for the most part, collected on the basis of authority, i.e. rules specified in the *Act*. The intent is to allow the health system to operate effectively. Please review sections 37-46 of *PHIA*. However, consent is also a key part of the *Act*. Depending on the circumstances, consent may be express or implied and a custodian must follow the rules of consent found in sections 23-28 of *PHIA*.

Sections 29-50 of *PHIA* covers all the requirements regarding collection, use and disclosure.

Access and Correction of Personal Health Information

Under section 52(1) of *PHIA* an individual has a right to access a record containing their personal health information that is in the custody or under the control of a custodian. Custodians must respond within 60 days of receiving a request to access personal health information as per section 55.

A custodian can respond and grant access to the record, refuse access to the record or advise that the record does not exist. Should a custodian fail to respond to an access request for personal health information within the legislated timeframe, they will be considered to have refused the request for access and the individual requesting access may appeal that refusal to the Trial Division, Supreme Court of Newfoundland and Labrador or request a review by the Commissioner.

Under section 60 of *PHIA*, when an individual has been granted access to a record containing their personal health information and that individual believes that the record is inaccurate or incomplete, that person may request the custodian correct the information.

Please review sections 52-64 for more detail on access and correction of personal health information under *PHIA*.

Podcast Discussion on OIPC Cyber Attack Report

On May 23, 2023, our Office issued Report P-2023-001/PH-2023-002 outlining the results of our investigation into the 2021 Cyber Attack. In our last issue of this Newsletter, we offered custodians a number of takeaways and tips that came out of this Report.

Commissioner Harvey recently discussed our Office's Report in episode 19 of "Un-redacted, The Sask IPC Podcast" hosted by Information and Privacy Commissioner of Saskatchewan, Ron Kruzeniski. Part I focuses on Commissioner Harvey's employment history and general priorities for the OIPC in his term, while Part II discusses the Cyber Attack Report.

Increasing Access to Health Care Through Virtual Care Contract

The provincial government announced in a news release on November 20, 2023 that Newfoundland and Labrador Health Services (NL Health Services) will launch a new virtual care solution this fall that will increase access to health care for rural areas and residents who do not have a primary care provider.

The virtual care service will include:

- virtual primary care for residents who do not have a primary care provider and have registered on Patient Connect. This access will be through a virtual physician available Monday to Friday 8:00 a.m. to 8:00 p.m.;

- a virtual emergency room that will ensure virtual physician coverage 24 hours per day, seven days per week to emergency departments in select rural health care facilities that do not have local physician coverage; and

- other needed physician coverage such as urgent care centres.

A contract valued at $11 million annually has been awarded to Teladoc to provide virtual technology, as well as physician coverage for two years.

The service will begin with the launch of the Virtual Emergency Room at the Dr. Y. K. Jeon Kittiwake Health Centre in New-Wes-Valley this week, and will expand to other communities in the following months.

Residents who are registered through Patient Connect or other provincial wait lists and have a valid MCP number will receive a letter in the mail informing them of how they can access the virtual care service. Residents who do not have a primary care provider and who have not registered for Patient Connect can do so at https://patientconnect.nlchi.nl.ca or via telephone at 1-833-913-4679.

More information on the virtual care service can be found at virtualcarenl.ca.

Searching for Personal Health Information

Earlier this year, Deputy Commissioner Diane Aldridge, at the Saskatchewan Office of the Information and Privacy Commissioner wrote a blog post, “The Search for Personal Health Information” which can be viewed in full here.

While the governing legislation in Saskatchewan, the *Health Information Protection Act* (*HIPA*) is slightly different with different definitions from NL’s *Personal Health Information Act* (*PHIA*), many of the points made regarding searching for personal health information are valid and worth reviewing.

The right of access by an individual extends to all personal health information that is in the custody or under the control of the custodian regardless of who created it, where it came from, how old it is or how it is stored. All records, in any form, that are responsive to the request, must be identified, located, retrieved and ready for release within 60 calendar days under *PHIA*.

Records may be in paper or electronic form whether found in a file drawer or in an electronic health record (EHR). Electronic or digital records include electronic documents such as word-processed documents, spreadsheets, email, digital photographs, scanned images and electronic data, such as information stored in databases or in registries or in rarer cases, back-up tapes.

Regardless of the medium, a thorough search needs to be conducted. As long as records have not been destroyed, access rights of the individual remain intact, and records need to be produced wherever they reside.

An access request for personal health information could be vague because an applicant lacks knowledge of a custodian's programs or operations or the type of health records that may exist. A large or vague request could be challenging for a large custodian, such as NL Health Services, and this is why communicating with an applicant early on in the request process is important to help clarify the request and possibly narrow a request where appropriate.

The responsibility to maintain records may fall to many different individuals at different times resulting in records being temporarily retained on a unit, in individual employee's offices, managed off-site by an information management service provider or put into storage while waiting to be culled. Also, a search at one time may reveal responsive records, but not necessarily all. Patient care is not static; therefore, new responsive records are always being generated.

Deputy Commissioner Aldridge's advice was to start with a search strategy by talking to the 'people in the know' before proceeding (e.g., record or health information managers). As well, she advised not to forget to document your search strategy and keep details of the actual search!

Reminder – Use of Email for Communicating Personal Health Information

While email may be a useful means of communicating personal health information to patients, it also involves an element of risk. It is ultimately the responsibility of custodians to safeguard personal health information in its custody or control. Responsibility of safeguarding personal health information cannot be transferred to an individual or patient by having them sign a consent form or disclaimer to accept the risks associated with electronic communications.

Section 15 of *PHIA* requires that a custodian take reasonable steps to ensure that the personal health information in its custody or control is protected against theft; loss; unauthorized access, use or disclosure; and unauthorized copying or modification. It also mandates that records containing personal health information be retained, transferred and disposed of in a secure manner.

Following are possible risks when sending electronic communications containing personal health information.

- **Interception:** if an account or device is shared by multiple people, the wrong recipient may read the message.
- **Misdirection:** patients may have similar names or email account addresses and a message may be sent to the wrong individual.
- **Alteration:** a patient may alter test results communicated by email and then send the results to another health care provider.
- **Loss:** health information could be lost if a service provider goes out of business or is taken over by another entity or if there is a security breach.
- **Inference:** the name and nature of a health care provider on its own may reveal health information of an individual should another person have access to or see notifications on a patient's device.

Following are some useful tips if a custodian must send an email containing personal health information.

- Limits
  - Limit the amount of personal health information being sent to only what is necessary.
  - Ensure that no personal health information is in the subject line of the email.
  - Only place essential information in the body of the email.
  - Personal health information should be sent as an encrypted attachment.
  - Whenever possible, reduce the amount of sensitive information in the body of the email. For example, rather than disclosing a patient's prognosis or diagnosis in an email, instead refer generally to the contents – "a test" or a "procedure" and ask the recipient to refer to the encrypted attachment for further information.
- Security
  - Ensure that personal health information is sent as a secure, locked (e.g. .pdf) attachment which requires a password to open.
  - Communicate the password to the recipient using a separate method.
  - Use a professional, as opposed to personal, web-based, email account to send the email. Personal accounts usually have weaker security and may be more susceptible to compromise.
- Verification
  - Verify the email address with the intended recipient(s) and re-check the email addresses, cc and bcc fields and attachments before sending.
  - Autocomplete or autofill options should be turned off to avoid errors.
  - Read/received/delivery receipts should be used where possible.
  - Add a disclaimer to your signature that indicates that the email is confidential and intended only for the intended recipient. It should also instruct anyone who receives the email in error to delete or shred the misdirected mail and notify the sender.
- Maintain Copies
  - Copies of the email and attachments should be maintained in the client file. The date, time, and addressee of the email should be apparent.

Please review our two guidance pieces on this topic – Sending Personal Health Information Via Email Quick Tips and Use of Email for Communicating Personal Health Information.

Breach Notifications

Between August 1, 2023 and October 31, 2023, OIPC received five breach notifications from five different custodians. This is a decrease from the seven breaches reported during the previous quarter. The largest breach was one where an email was sent without using Bcc and two of the other breaches involved phone messages being left to incorrect phone numbers.

We would like to remind custodians that OIPC can offer *PHIA* training that is 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.