SAFEGUARD

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

Volume 5, Issue 4 November 2021

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:

Privacy and the Cyberattack on the NL Health System

Anyone who believes their personal information or personal health information may have been accessed or stolen as a result of the cyberattack on our health system has a right to file a complaint with the NL OIPC. We wish to advise, however, that the Information and Privacy Commissioner has already decided to launch a privacy investigation. Unless you believe there are very specific circumstances particular to your own case that would warrant an individual complaint, it won't be necessary for individuals to file a complaint. If you have any questions or aren't sure if you should file an individual complaint, feel free to contact our Office to discuss further.

For more information about the cyberattack and how it has impacted the health system and the personal information of residents, it is recommended that you refer to the resources prepared by the Department of Health and Community Services or use the Department's toll free number (1-833-718-3021).

What is a Cyberattack?

We have all seen the news of the cyberattack that impacted the health sector. While it is too early to discuss specific details of this particular attack, we wanted to provide general information about such attacks and remind you of the steps the Department has identified to help you protect yourself.

The Canadian Centre for Cyber Security (Cyber Centre) is Canada's authority on cyber security. The Cyber Centre defines a cyberattack as the "use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device."

The Cyber Centre issued a publication titled, National Cyber Threat Assessment 2020, and it contains a few key judgements of particular interest, as they may help readers better understand the threat environment facing entities today:

- *The number of cyber threat actors is rising, and they are becoming more sophisticated. The commercial sale of cyber tools coupled with a global pool of talent has resulted in more threat actors and more sophisticated threat activity. Illegal online markets for cyber tools and services have also allowed cybercriminals to conduct more complex and sophisticated campaigns.*
- *Cybercrime continues to be the cyber threat that is most likely to affect Canadians and Canadian organizations. We assess that, almost certainly, over the next two years, Canadians and Canadian organizations will continue to face online fraud and attempts to steal personal, financial, and corporate information.*

The Department has provided a list of resources of how you can protect your information; see their FAQ page for the cyberattack. The Privacy Commissioner of Canada also has Identity Theft resources and the Government of Canada has tips on cyber safety on its Get Cyber Safe website. While not a Canadian resource, the Australian Cyber Security Centre has great tips on how to protect yourself, as well as some common warning signs that your identity may be compromised. And for anyone looking for more information on staying safe online and securing accounts, the National Cyber Security Alliance has a number of resources that may assist.

Report PH-2021-001 Learnings

Report PH-2021-001 addressed complaints against two custodians involved in a single transaction. The complainant had concerns with both the disclosure by one custodian, a Regional Health Authority (RHA), and the use of the disclosed information by another custodian, WorkplaceNL. The Commissioner found that there had been an improper disclosure of the Complainant's personal health information by the RHA, but not an improper use of that information by WorkplaceNL. The RHA should not have disclosed some of the information it did, when it disclosed it, because WorkplaceNL did not ask for it; its request was narrower than the information provided to it. But once it had this extra information, WorkplaceNL found it relevant and was legally authorized to use it. WorkplaceNL's legal powers to use information to discharge its mandate are quite broad. While it may seem counter-intuitive, WorkplaceNL's broad power to use information in its possession does not change the fact that the RHA should not have disclosed it; nor does the fact that the RHA should not have disclosed the information change the fact that WorkplaceNL was authorized to use it.

Under section 13 of *PHIA*, custodians are required to have policies and procedures to facilitate compliance with the Act. In this investigation, the Custodian disclosing the information revised its Disclosure of Information Policy to provide a clearer process for responding to requests for records of personal health information. For example, the new guidelines direct staff to date stamp the request to create a record of when the request was received; to review the request to ensure there is consent from the patient (and if consent has not been received, to not proceed before contacting a manager); to search for records and verify the request is for the correct patient; and to only print those records that have been requested. The guidelines advise not to provide information that has not been specifically requested. The guidelines also state to retain a copy of the request, the completed consent form and cover letter.

Requests for Correction of Personal Health Information

While access to personal health information was discussed in the August 2021 edition of Safeguard, custodians are reminded that clients are also able to request corrections to their personal health information.

When an individual who has been granted access to their personal health information (PHI) identifies incorrect PHI within their record, they are able to request a correction of information as per Section 60(1) of *PHIA*. This request can be submitted in writing or verbally at no charge to the individual. It is the responsibility of the custodian to take reasonable steps to confirm the individual's identity in order to process a request to correct PHI.

A custodian will require sufficient information to allow for record retrieval with reasonable effort; for example, this may include name, birth date, address, and/or MCP or other unique identifier(s).

Timely Response

A custodian must respond to a PHI correction request no more than 30 days* after receiving it. However, a custodian may extend the time limit by an additional 30 days* where

- meeting the original due date would unreasonably interfere with the operations of the custodian, or
- the information that is the subject of the request for correction is located in numerous records so that the request cannot be completed within the original 30 days*.

Should a custodian extend the original response time by 30 days*, the custodian must give the requestor written notice of the extension along with reasons for the extension. A custodian must respond to the individual's request as soon as possible and no later than the expiration of the extended time limit.

The custodian must grant the request for correction where the individual has demonstrated that the record is incomplete or inaccurate for the purposes of the information and gives the custodian the information necessary to make the correction.

Making the Correction

When a request for correction is granted, the custodian must make the correction and provide written notification to the individual that it has been made as per Section 63 of *PHIA*. The custodian must also provide written notice of the requested correction, to the extent reasonably possible, to those whom the custodian has disclosed the information within the 12 month period immediately preceding the request, unless the custodian reasonably believes that the correction will not impact the ongoing provision of health care or other benefits.

Refusing the Correction

A custodian may refuse a request to correct personal health information if the record was not originally created by the custodian and the custodian does not have sufficient knowledge, expertise and authority to correct the information. The OIPC discussed such a refusal in Report AH-2020-001.

A custodian may also refuse a request for correction where the information consists of a professional opinion or observation the custodian has made in good faith about the individual or the custodian believes on reasonable grounds that the request is frivolous, vexatious or made in bad faith.

When a custodian refuses a request to correct PHI, the custodian must annotate the personal health information with the correction that was requested and not made. Where practical, the custodian must also notify those to whom the custodian has disclosed the information within the 12 month period immediately preceding the request for correction of the annotation, unless the custodian reasonably believes that the correction will not impact the ongoing provision of health care or other benefits. OIPC discussed Section 63(2)(a) of *PHIA* in Report AH-2014-001.

Recourse

When a request to correct PHI is refused, the custodian must provide the requestor with a written notice outlining the correction that the custodian refused to make, the reasons for the refusal and the right of the individual to appeal the refusal to the Trial Division or request a review by the Commissioner of Information and Privacy.

Learnings from OIPC NL *PHIA* Access Reports

Report AH-2014-001 is the first Report in which OIPC NL examined the matter of a correction request under *PHIA* in detail. In that case, the individual requested that a clinical report be removed from a medical file; the custodian appropriately treated this as a correction request. There is no provision in *PHIA* that authorizes the custodian to destroy medical information in this particular circumstance.

The Report assessed the correction request using a two-step process initially used by OIPC Alberta; the first step considers whether any of the information at issue consists of "a professional opinion or observation". The second step is to examine any remaining information in the disputed record that does not consist of professional opinion or observation, and determine whether in that remaining information there are errors or omissions of fact that may be subject to correction.

Report AH-2017-001 examined other, informal ways to access one's own personal health information. A custodian responded to a request for information by processing the application under their routine file release process. The applicant was not satisfied that the custodian had not processed the information under the Act. The Report examined if the request should have been treated as a *PHIA* request or an *ATIPPA, 2015* request. The Commissioner recommended that the custodian treat all requests for medical information as a request under *PHIA*, even if they continued to use a routine file release process.

Report AH-2020-001 examined a request for correction involving information created by another custodian. The Commissioner reminded the custodian of its obligation to annotate the record with the fact that a correction request had been received and the reason for the refusal.

*Definition of "days" falls under the *Interpretation Act*, Section 22(K).

Complaints and Breach Notifications

*Please note that our breach statistics have returned to a standard three month time frame, as they do in our *ATIPPA, 2015* newsletter Above Board. The cyberattack breach reports were received after October 31st and will be included in the February 2022 edition of Safeguard.

Between August 1 – October 31, 2021, OIPC received five breach notifications related to *PHIA*. The five breaches were reported by two different Regional Health Authorities and a health care professional. Two involved misdirected mail and one involved a brief exposure to an appointment list. One was an intentional breach by a staff member seeking information about themselves; when they contacted a clinic to find out if results were available and was told they were not, they presented at the clinic and instigated a search of paper files for their own results. The final breach occurred when a health care professional discovered that a patient was using someone else's MCP card; the professional notified the affected patient, the insurer, and other health care professionals who were in the individual's circle of care.

Six new privacy complaints and one access complaint were received during this timeframe, involving five different custodians. Two complaints involve e-mail notifications that did not blind copy, allowing all those receiving the e-mail to see the complete distribution list and reply to the entire group. OIPC has developed both Quick Tips and a more detailed guidance piece for custodians considering transmitting personal health information using e-mail.