

Annual Report

2021 – 2022



Northwest Territories



OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER

NORTHWEST TERRITORIES

If you would like this information in another official language, call us.

English

Si vous voulez ces informations dans une autre langue officielle, contactez-nous.

French

Kĩspin ki nitawih̄tĩn ē nĩhĩyawih̄k ōma ācimōwin, tipwāsinān.

Cree

Tłjchq yati k'ǰǰ Dı wegodi newq dè, gots'o gonede.

Tłjchq

ʔenht'is Dēne Sųłĩné yati t'a huts'elkēr xa beyáyati theʔa ʔat'e, nuwe ts'ēn yófti.

Chipewyan

Edı gondı dehgáh got'je zhatié k'ǰedat'éh enahddhę nıde naxets'ę edahfi.

South Slavey

K'áhshó got'jne xada k'é hederı ʔedjhtl'é yerınwę nıde dúle.

North Slavey

Jii gwandak izhii ginjik vat'atr'ijáhch'uu zhit yinohtan ji', diits'at ginohkhii.

Gwich'in

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.

Inuvialuktun

Ĉ'bdġ ǱǱ^{sb}Δ^c ΛϳLJΔ^{rc} Δ^{sb}Ǳġ^c ^{sb}ʔLǱǱ^b, Ɓ^{rc}Ǳ^a Ɓ^c Ɓ^{sb}ċ^a Ǳ^{sb}Ǳ^c.

Inuktitut

Hapkua titiqqat pijumagupkit Inuinnaqtun, uvaptinnut hivajarlutit.

Inuinnaqtun

Office of the Information & Privacy Commissioner : (867) 669-0976
Commissariat à l'information et à la protection de la vie privée : 867-669-0976



July 1, 2022

The Honourable Frederick Blake
Speaker of the Legislative Assembly
PO Box 1320
Yellowknife, NT
X1A 2L9

Dear Mr. Speaker,

Pursuant to section 68 of the *Access to Information and Protection of Privacy Act* and section 173 of the *Health Information Act*, I have the honour to submit my Annual Report to the Legislative Assembly of the Northwest Territories for the period from April 1, 2021, to March 31, 2022.

Your truly,

Andrew E. Fox
Information and Privacy Commissioner
of the Northwest Territories

/af

Table of Contents

<u>Commissioner's Message</u>	Page 1
<u>Financial Report</u>	Page 3
<u>Office of the Information and Privacy Commissioner and Enabling Legislation</u>	Page 5
The Access to Information and Protection of Privacy Act The Health Information Act The Information and Privacy Commissioner	
<u>The Year in Review</u>	Page 8
Overview of the Numbers (ATIPPA and HIA) Access to Information and Protection of Privacy Act <i><u>Review Reports</u></i> <i><u>Time Extension Requests</u></i> <i><u>Review of Draft Legislation</u></i> <i><u>Timelines in ATIPPA</u></i> Health Information Act <i><u>Review Reports</u></i> <i><u>Increase in Privacy Breaches</u></i> <i><u>Recurring Issues in Privacy Breaches</u></i> <i><u>Privacy Impact Assessments</u></i>	
<u>Interjurisdiction Activity</u>	Page 20
<u>Final Thoughts</u>	Page 21
<u>Summary of Recommendations</u>	Page 22
<u>Contact Us</u>	Page 23

Commissioner's Message



I am pleased to present this Annual Report for the period April 1, 2021, to March 31, 2022, my second since being appointed as the Information and Privacy Commissioner on November 23, 2020. It has been a busy year! The number of new files increased significantly over the previous year, and this appears to be a continuing trend. The largest increase has come from contraventions of the *Health Information Act*, (HIA) but there have been increases in most categories of matters this office deals with. We have much to keep our new Investigator busy. Welcome to Kristen Luce Vivian!

Perhaps the most significant milestone this fiscal year was the coming into force on July 30, 2021, of the amendments to the *Access to Information and Protection of Privacy Act* (ATIPPA). The amendments include several significant changes:

- Extensions of time to respond to an access to information request now require prior authorization to extend beyond 20 additional business days.
- For responses to access to information requests, some exceptions to disclosure have been removed.
- Public bodies must now report a privacy breach event to the Office of the Information and Privacy Commissioner in the event of a “material breach” and must report a privacy breach to the individual if the breach creates a ‘real risk of significant harm to the individual.’
- Public bodies must disclose information to the public or to an affected group or individual about a risk of significant harm to the environment or to health or safety of the public, or if disclosure is for any other reason clearly in the public interest.
- The Commissioner now has authority to institute a review without a formal complaint being received from an individual.
- Privacy Impact Assessments are now required in the development of an enactment, system, project, program, or service that involves the collection, use or disclosure of personal information. This reflects a policy requirement established in 2019.

A striking feature of this year’s work was the sheer volume of new matters. We opened 95 new ATIPPA files, an increase from 75 files in the previous year, and 234 new HIA files, a large increase from 87 the previous year. Fifty five of those new HIA files relate to privacy breaches involving the COVID Secretariat.¹ This increase follows a long-term trend which has seen a sixfold increase

¹ This is a unit located within the Department of Health and Social Services. Some of these breaches occurred in the previous year but were reported late.

in files opened in the OIPC from 2011/12 to 2019/20.² The increasing file load raises questions regarding the efficacy of privacy protection policies and processes governing health information custodians and also raises concerns about the resourcing of access to information and privacy protection functions, both for public bodies and for the OIPC. The increase in new matters is likely due to an increased number of privacy breaches as well as more thorough reporting. I anticipate the number of privacy impact assessments submitted to our office will continue to increase. We will be monitoring the volume and type of new matters going forward.

During the pandemic public access to government information and services on-line has increased. In November 2021, the Government of the Northwest Territories (GNWT) expanded its on-line services with the new eServices Portal, facilitating applications for registration and renewal of health care insurance cards, driver and vehicle registration, purchase of fishing licenses, applications for student financial assistance, and inquiries to the Apprenticeship, Trades and Occupation Certification. As well, the GNWT has been providing on-line access to Personal Vaccination Certificates as part of the public health response to the COVID-19 pandemic.

New ways of sharing information and bringing services to people can benefit society. However, new technologies also come with risk. Given the ever-present threat of unwanted surveillance and data theft, vigilance is essential. As the online environment changes and as the government adds online services, security measures must continue to evolve to protect personal information from existing and new threats to privacy and security. Privacy Impact Assessments (PIAs) are an important tool to help government avoid or mitigate risks, and they are now required under both the HIA and the ATIPPA.

Public health directives on isolation required working from home for extended periods posing a challenge to records handling. Many of us worked from home for the first time, and some even started new jobs in that environment; indeed, our new Investigator began with us while the pandemic work-from-home protocols were in place earlier this year. Though we struggle with the file load, we have been able to adapt and to work effectively and maintain stable services to the public even when working remotely. Because of the pandemic, work travel has been avoided. But, we have been able to attend web-based conferences and take advantage of other e-learning opportunities increasingly offered online, and I expect we will continue to utilize a combination of in-person and online facilities as we go forward. We look forward to another busy year.

² This was identified most recently in the Legislative Assembly's Standing Committee on Government Operations' Report on the Review of the 2020-21 Annual Report of the IPC. See page 2.

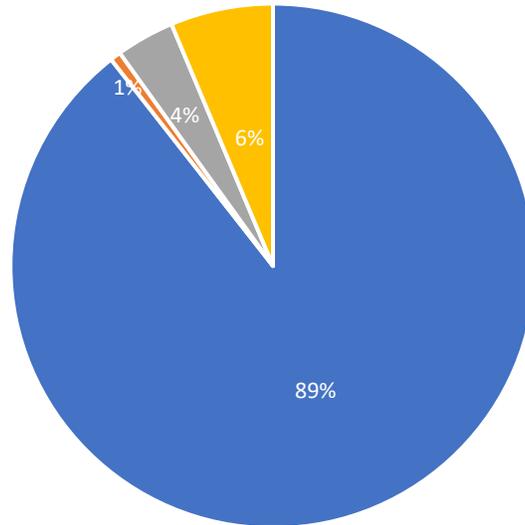
Financial Report

The total amount spent to operate the Office of the Information and Privacy Commissioner (OIPC) of the Northwest Territories for the fiscal year 2021/2022 was \$609,279.53. A detailed breakdown is outlined in the charts on the next page.

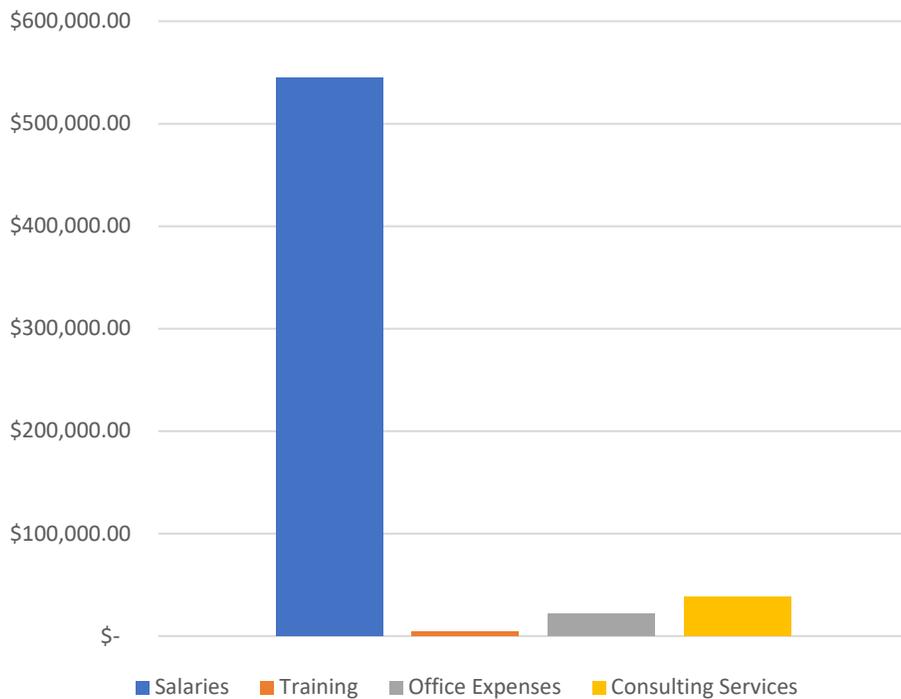
The administration of the OIPC budget was again uneventful. Our total operating budget was \$753,000.00 and we returned \$143,720.47 unspent to the Legislative Assembly. There were a few variances between actual and budgeted amounts:

1. Funds returned to the GNWT were for salaries. We spent less than anticipated for a few reasons. First, it took longer than anticipated to staff the new Investigator position, filled in January 2022. Second, existing staff job descriptions needed updating and it took longer than anticipated to finalize and complete the entire formal revaluation process, affecting the Office Manager (now the Investigation, Communication, and Finance Coordinator) and the Assistant Information and Privacy Commissioner positions. The impacts of these changes will be felt in the 2022-23 fiscal year budget.
2. There were additional costs for home-office set-up during isolation periods. These were one-time costs not expected to be repeated.
3. There was continued use of consultants to help with the backlog of Privacy Impact Assessments and some investigations. These are now up to date.
4. Professional development and training for staff is a continuing expense. The Federal, Provincial and Territorial Information and Privacy Commissioners delivered two online 'Investigator Conferences' for a nominal fee. This was a wonderful opportunity for smaller offices like our own to gain insight and expert advice from larger provincial and federal offices which have more and often specialized resources. These were useful professional development activities and are expected to continue annually. A small portion of our annual budget will continue to support other learning opportunities for staff and management, including access to reference resources and relevant academic and professional training.
5. Due to COVID-19 travel restrictions, there was no work-related travel again this year. Conferences and other learning opportunities are returning to in-person attendance; for instance, the annual federal, provincial, and territorial privacy commissioner's meeting this year is being hosted in-person in St. John's, Newfoundland and Labrador.

**Office of the Information and Privacy
Commissioner of the Northwest Territories
2021 / 2022 Expenses**



■ Salaries ■ Training ■ Office Expenses ■ Consulting Services



■ Salaries ■ Training ■ Office Expenses ■ Consulting Services

Office of the Information and Privacy Commissioner and Enabling Legislation

The Access to Information and Protection of Privacy Act

The *Access to Information and Protection of Privacy Act*³ (ATIPPA), applies to the departments, branches, and offices of the government of the Northwest Territories, plus 22 agencies, boards, commissions, corporations, and other public bodies designated in the regulations to the Act.⁴ With the amendments that came into force in 2021, municipalities may be designated as public bodies by regulation.⁵

The ATIPPA enshrines four key rights and obligations:

- the right of the public to have access to records in the custody or control of a public body, subject to limited and specific exceptions;
- the right of individuals to have access to their own personal information held by public bodies and to request corrections to their own personal information;
- the obligation of public bodies to protect the privacy of individuals by preventing the unauthorized collection, use or disclosure of personal information; and
- the right to request independent review of public bodies' decisions regarding access to government records or regarding the collection, use, disclosure, or correction of personal information.

The Act has two fundamental purposes: to provide access for the public to government records and to provide protection for individuals' privacy by controlling the government's collection, use, and disclosure of personal information. Part 1 of the Act sets out the right of the public to access records held by public bodies and outlines the process for members of the public to obtain access to such records. Part 2 governs when and how public bodies can collect, use, or disclose individuals' personal information.

The Commissioner provides independent review of public bodies' decisions and actions under both Parts. After investigating the facts and receiving representations from the applicant or complainant, from the public body and from any relevant third parties, the Commissioner will issue a review report, which will contain an order and may contain additional terms and

³ SNWT 1994, c 20.

⁴ Subject to limitations and exceptions set under ATIPPA or other legislation.

⁵ No communities have yet been designated.

conditions. A public body is required to comply with a Commissioner's order, subject to appeal to the Supreme Court of the Northwest Territories

Access to information and protection of privacy are both essential to ensure transparency and accountability of government -- vital elements for a healthy and effective democracy. Recent substantial amendments added privacy breach response and privacy impact assessment requirements to the Act.⁶

Although access to government records is a legal right, it is not unfettered: there are statutory exceptions – some mandatory, some discretionary – that permit public bodies to withhold all or part of some records. Decisions made in a response to an access to information request can involve potentially complex issues regarding the proper extent of disclosure and the proper application of statutory exceptions that may require or permit information to be withheld. Independent oversight helps to ensure that public bodies apply the Act correctly. Oversight also helps assure applicants that their rights are being upheld.

The Health Information Act

The *Health Information Act*⁷ (*HIA*) governs the collection, use and disclosure of personal health information, recognizing both the right of individuals to access and protect their personal health information and the need of health information custodians to collect, use and disclose personal health information to support, manage and provide health care. The *HIA* regulates health information custodians in both the public and the private sectors, including the Department of Health and Social Services, the Northwest Territories Health and Social Services Authority, the Hay River Health and Social Services Authority, the Tłı̄ch̄q Community Services Agency, and private physicians and pharmacists operating in the Northwest Territories.

The *HIA* establishes the duty for health information custodians to take reasonable steps to protect the confidentiality and security of individuals' personal health information. It also gives patients the right to limit the collection, use and disclosure of their personal health information, and to put conditions on who has access to their personal health records and what personal health information may be accessed. Governing these provisions is the principle that a health service provider's access to an individual's personal health information should be limited to the information that health service provider "needs to know" to do their job.

The *HIA* also requires health information custodians to notify affected individuals if personal health information is used or disclosed other than as permitted by the *Act*, or if it is stolen, lost, altered, or improperly destroyed. Notice to the Commissioner is required in the event of an unauthorized disclosure, or in the event of unauthorized use, loss, or destruction where there is a reasonable risk of harm to an individual. In such circumstances, the Commissioner may initiate an investigation on his own initiative or upon the request of an individual who believes their personal health information was collected, used, or disclosed in contravention of the *Act*.

⁶ Substantial amendments were passed in SNWT 2019 c.8 and came into force on July 30, 2021.

⁷ SNWT 2014, c 2.

After conducting a review, the Commissioner will prepare a report and may make recommendations to the health information custodian. The custodian must notify the Commissioner of the custodian's decision to follow or not to follow the recommendation(s) within 30 days of receiving a report and must comply with a decision made to follow the Commissioner's recommendation within 45 days after giving notice of the decision to the Commissioner. Applicants who are unsatisfied with a health information custodian's decision regarding a recommendation may appeal the decision to the Supreme Court.

The Information and Privacy Commissioner

The Information and Privacy Commissioner is a Statutory Officer of the Legislative Assembly of the Northwest Territories, appointed by the Legislative Assembly for a five-year term. The Commissioner operates independently of the government and reports directly to the Legislative Assembly.

The Commissioner has powers, duties and functions set out under the *Access to Information and Protection of Privacy Act (ATIPPA)* and the *Health Information Act (HIA)* which are carried out through the Office of the Information and Privacy Commissioner (OIPC). In addition to dealing with complaints about access to information responses and breaches of privacy, the Commissioner also provides comment regarding Privacy Impact Assessments (PIAs) that are submitted to the Office of the Information and Privacy Commissioner by public bodies. PIAs are generally required when a public body or health information custodian is developing a new system, project, program, or service involving the collection, use or disclosure of personal information or personal health information. PIAs are a key planning tool to ensure that the privacy implications of proposed policies or programs, etc., are considered at an early stage. A PIA helps confirm where plans align with legislative requirements, and where there are gaps and weaknesses that requiring resolution *before* implementation.

PIAs have been required under the HIA since it came into force in 2015 and they are now required under the ATIPPA⁸ and the GNWT's Protection of Privacy Policy 82.10.⁹ In addition to PIA's, the Commissioner may also review and comment on proposed legislation in regard to possible implications for privacy protection or access to government information.

⁸ Section 42.1 came into force with the other amendments on July 31, 2021.

⁹ This policy has been in place since August 2019.

The Year in Review

The Office of the Information and Privacy Commissioner opened a total of 329 files in the fiscal year 2021/2022. Of these, 95 were matters within the scope of the *Access to Information and Protection of Privacy Act* and the remaining 234 are matters governed by the *Health Information Act*.

Overview of the Numbers

Access to Information and Protection of Privacy Act (ATIPPA)

The OIPC opened 95 files under the *Access to Information and Protection of Privacy Act* between April 1, 2021, and March 31, 2022:

Requests for Review – Access to information and redactions	17
Requests for Review – Delays and extensions taken	18
Requests for Review – 3 rd party requests	9
Request for Review - Privacy issues and complaints	18
Request from Public Body - Extension of time to respond	13
Request from Public Body - Disregard an ATIPP request	1
Notification from Public Body - Breach of privacy	13
Consultations/Comments – Acts, legislations, bills	6

Health Information Act (HIA)

The OIPC opened 234 files under the *Health Information Act* between April 1, 2021, and March 31, 2022:

Notifications from Public Body - Breach of privacy	206
Request for Review – Privacy Issues and complaints	4
Comments – Privacy impact assessments	15
Comments – Health policies, acts, processes	8
Miscellaneous and Administrative	1

Access to Information and Protection of Privacy Act

Section 68 of the *ATIPPA* requires the Annual Report to provide an assessment of the effectiveness of the Act and to report on the activities of the Commissioner and any instances where recommendations of the Commissioner made in a review were not followed. The following matters are relevant to these requirements, and in some cases I have made recommendations for consideration by the Legislative Assembly.

Review Reports

Our office issued 27 review reports under the *Access to Information and Protection of Privacy Act (ATIPPA)* in 2021/2022. Ten reports reviewed public bodies' responses to access to information requests. Ten reports dealt with public bodies' requests for extensions of time to respond to access to information requests. Seven reports reviewed whether personal information was collected, used, or disclosed without legal authorization.

Review reports are freely available on-line at <https://www.canlii.org/en/nt/ntipic/>.¹⁰

Prior to the amendments to the *ATIPPA* coming into force on July 30, 2021, the Commissioner could conduct reviews and make recommendations in regard to public bodies' responses to access to information requests and to instances of unauthorized collection, use, disclosure, or loss of personal information. As of July 30, 2021, the Commissioner can now issue orders at the conclusion of reviews. These orders are binding on public bodies. To monitor compliance, my office has developed a practice of imposing a term in each order requiring the public body to report back to our office on its compliance activity. This should assist my office to determine if there are any issues with the implementation of, or compliance with, any orders. Thus far we have not identified any compliance issues.

The Commissioner may still make formal recommendations for a public body's consideration under Division E of Part 2 of *ATIPPA*. This is an entirely new Division that deals with instances of data breach involving personal information. If a privacy breach is "material"¹¹ the head of a public body must provide a report to the Commissioner about the breach of privacy. If the Commissioner determines the privacy breach creates a "real risk of significant harm" to one or more individuals, the Commissioner may recommend the head take steps to provide further notice, to limit the consequences of a breach, or to prevent further breaches of privacy. The head of a public body will have to decide whether to follow any recommendation and will have to report to the Commissioner regarding the implementation of any accepted recommendations. My office did not receive a notice or report regarding a data breach under Division E.

¹⁰ Past years' decisions are also available on-line on this free public database.

¹¹ The Act does not define this term but there are factors to consider set out in subsection 49.9(2).

Time Extension Requests

This is a new category of review report. Prior to July 30, 2021, public bodies could extend the time to respond to an access request for a “reasonable period.” Extensions were subject to review by the Commissioner if an individual applicant requested. Formal review reports for such situations were infrequent. Unless an applicant complained to our office about an unreasonable delay, the OIPC would not be involved in tracking or authorizing time extensions. If there was a complaint of a delay, a preliminary inquiry by the Commissioner would often lead to a resolution of the problem without need of a review.

Since July 30, 2021, the timelines, and the process for extending time periods have changed. Public bodies have an initial 20 business days to respond to an access to information request and can extend this period once for up to 20 business days if the conditions prescribed in section 11(1) are satisfied. Any further extension requires authorization by the Commissioner. An application for authorization must be submitted prior to expiration of the existing time period. If the time period expires before the public body provides a response the Act deems this to be a refusal to respond.¹²

Time extensions for third-party consultation

My office issued ten review reports after July 30, 2021, each granting time extensions to accommodate public bodies’ consultation with third parties, prior to providing a response to the access to information requests. The third-party consultation framework under ATIPPA provides a period of 55 business days to complete third-party consultation.¹³ In every case this will exceed the 20 business-day extension available under subparagraph 11(1)(c), and therefore requires authorization by the Commissioner under section 11.1. Barring any changes to the Act, we expect to review a substantial number of extension requests for third-party consultation.

Where the Act requires third-party consultation there is no reasonable basis for the IPC to deny an authorization. The authorization process is essentially a ‘rubber stamp’ where third-party consultation is required. In my view, this situation warrants further consideration.

Recommendation 1: *The legislative assembly should consider amending the ATIPPA to allow a public body to extend the time once for the period required to complete third-party consultation without authorization by the IPC. For subsequent extensions, public bodies should continue to seek authorization from the IPC.*

Time extensions to prevent unreasonable interference with the operations of a public body

Subparagraph 11(1)(b) allows an extension of time for the public body to respond to an access request when a large number of records is requested or must be searched to identify the record requested and meeting the time limit would unreasonably interfere with the operations of the public body. Prior to the July 30, 2021, amendment, public bodies often relied on this subsection

¹² See section 8(2) of the *Access to Information and Protection of Privacy Act*

¹³ This includes a 40 business-day period to render a decision and a 15 business-day appeal period.

to grant themselves extensions of time to respond to an access request during the preparation of a response, sometimes more than once. A public body may now only grant itself one extension of 20 business days and must seek authorization from the Commissioner for any further extension. The threshold issue squarely engages the capacity of a public body to respond reasonably to access to information requests, particularly when a request places additional demand on the public body.

The Government of the Northwest Territories (GNWT) has created the Access and Privacy Office (APO) to provide support to all GNWT departments¹⁴ to fulfill their ATIPPA obligations. Through this “Centralized Service Model” the GNWT has assigned many of the public bodies’ access to information functions to the APO. This promotes and concentrates expertise within that office, helping to bring critical knowledge and experience and efficiency to the access to information process. This appears to be a good service model and my office has already seen the positive effects of this initiative.

Capacity remains an issue. The government recently stated that “Initial funding related to the implementation of a centralized ATIPP unit for the GNWT (the APO) was provided to the Department of Justice (DOJ) to ensure that there was consistency across government for the processing of access to information requests under the ATIPP Act, and also ensure that there was sufficient capacity and expertise to process those requests efficiently and effectively.”¹⁵ This is a statement of intent; however, if funding does not actually provide sufficient human and other resources, the APO will not be able to adequately support the government departments to discharge their statutory obligations.

Although the APO is the designated access to information coordinator¹⁶ for government departments, responding to an access request with the statutory framework remains the public bodies’ legal responsibility. I recently examined this issue in a review report addressing an application for an extension based on subparagraph 11(1)(b).¹⁷ I was advised that the APO has been short staffed for the last two years and that the public body had failed to provide its response within the statutory time three times on recent files. The public body was relying on the APO to do its assigned functions, even though it was apparent that the APO did not have the capacity. While each request for authorization must be reviewed on its own merits, it will likely be difficult for a public body to satisfy the requirements for an extension under subsection 11(1)(b) if the public body relies on a unit in another department to do the necessary work, and that unit is not staffed and resourced sufficiently to do that work. In my view, this situation warrants further attention.

¹⁴ And the Northwest Territories Housing Corporation

¹⁵ See Government of the Northwest Territories Response to Committee Report 5-19(2): Report of the Information and Privacy Commissioner of the Northwest Territories at page 2. Located at: https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf

¹⁶ Since October 27, 2020.

¹⁷ See 2022 NTIPC 10 (CanLII) <https://canlii.ca/t/jq3fd>

Recommendation 2: *Public bodies that rely on the APO to discharge their ATIPPA obligations should ensure, on an ongoing basis, that the APO is staffed and resourced to a level reasonably adequate to the task.*

Reviews of Draft Legislation

Pursuant to section 67(1)(c) of the ATIPPA, the Information and Privacy Commissioner may provide comments on the implications for privacy protection arising from proposed legislation. The Standing Committee on Government Operations sought the Commissioner's comments twice this past year: in regard to Bill 37, which proposed a few amendments to the ATIPPA, and in regard to Bill 39, *An Act to Amend the Post-Secondary Education Act*.

Bill 37 came into force on March 30, 2022, amending two definitions and repealing and replacing section 49.5 of ATIPPA. Section 49.5 provides jurisdiction for the Commissioner to prepare a report and make orders in the event of an unauthorized collection, use, or disclosure of an individual's personal information.

Bill 39 was given assent on March 31, 2022, with some changes to the sections creating post-secondary education advisory committees. Bill 39 proposed a number of amendments to the *Post-Secondary Education Act*, an Act passed by the 18th Assembly in 2019 but not yet in force. I provided comments about the creation of post-secondary education advisory committees and whether the records of such committees are intended to be subject to production under ATIPPA, or if they are intended to be subject to an exemption.

Timelines in ATIPPA

Prior to the amendments to ATIPPA coming into force on July 30, 2021, the Act stated a review must be completed within 180 days of receipt of a request for review.¹⁸ This period is now reduced to 90 business days.

While the OIPC supports the policy goal of providing an expeditious review process, adhering to a shortened deadline is difficult to achieve in practice. The average period to complete a review at that time was just over 12 months -- significantly more than 180 days. Our new Investigator came onboard in January 2022 and undoubtedly this will help. However, that position was approved in 2020 based on the file load increases that had already occurred in preceding years. While OIPC staffing has now increased from three to four people (including the Commissioner), the number of files coming into the office has doubled in the same period.

While my office will continue to work as thoroughly and efficiently as possible, it is unlikely that most reviews will be completed within 90 business days. I proceed on the basis that I do not lose jurisdiction if I take more than 90 business days to complete a review and make; to conclude

¹⁸ See section 31(3).

otherwise would fundamentally frustrate the objectives of the Act and the public's ability to seek a remedy through a review. While it may be useful for the Act to set a 'benchmark' timeline for completing a review, it would help clarify the review process if the Act expressly provided that the Commissioner could extend the period for completion of a review.

Recommendation 3: *The Legislative Assembly should consider amending the Access to Information and Protection of Privacy Act to expressly state the Information and Privacy Commissioner has discretion to extend the time required to complete a review. Such an amendment should include a requirement to give notice of an extension to all parties.*

Health Information Act

Review Reports

Our office issued three review reports under the *Health Information Act* this year. These reports, like those issued under the *Access to Information and Protection of Privacy Act*, are available online at <https://www.canlii.org/en/nt/ntipc/>.

Subparagraph 173(b) of the *Health Information Act* requires the Annual Report to report on recommendations that were made in a report to a health information custodian that were not accepted. This year, all recommendations made were accepted by the health information custodians, indicating that the recommendations will be followed.

Alternative Solutions

In part, the decrease in the number of reports reflects an increase in the use of alternative approaches to resolving matters. Conducting reviews and issuing review reports with recommendations to the custodian¹⁹ is one process. Another is to work with the health information custodian to address a matter using alternate dispute resolution process²⁰ or, even less formally, by providing comment and guidance and identifying relevant resources for consideration. This flexible approach continues to be well received by custodians and has led custodians to develop new measures to prevent privacy breaches and to respond better to breaches when they occur. I will continue to use this approach where appropriate.

Responding to Commissioner's Recommendations

At the conclusion of a review the Commissioner issues a report which may contain recommendations. After receiving a review report, a custodian has 30 days to decide whether to accept a recommendation and to notify the Commissioner of the decision.²¹ The Act deems a

¹⁹ On request by an individual under Section 134 or on the Commissioner's own initiative under section 137.

²⁰ Section 138.

²¹ Section 156.

failure to decide or to notify the Commissioner of the decision within 30 days as a decision not to follow the Commissioner's recommendations.

Despite this 'deeming' provision, there are often delays in responding to the Commissioner's recommendations. In one recent example,²² the Commissioner provided a review report containing eight recommendations to the custodian in May of 2020, but the custodian did not respond substantively until June 30, 2021. Reminder letters were sent to the custodian in the interim, and the custodian acknowledged the need for a response in September 2020. After nine more months the custodian accepted all the recommendations. The delay was attributed to operational challenges due to the pandemic. In future, we expect to see better adherence to the legal requirement to respond to recommendations within 30 days.

Once a recommendation is accepted, the Act requires the custodian to comply with the recommendation within 45 days following that decision. However, there is no statutory oversight of a custodian's implementation of an accepted recommendation. Our office does not have any authority or resources to conduct such oversight, nor is there any legal obligation for a custodian to report on the implementation of any accepted recommendations. In comparison, the amended ATIPPA section 49.14 creates just such an obligation.²³ In my view, it would be helpful to have a formal reporting process on the implementation of recommendations.

Recommendation 4: *The government should consider implementing a policy, or the Legislative Assembly should consider amending the Health Information Act, to require health information custodians to report to the Commissioner regarding the implementation of accepted recommendations.*

Increasing Privacy Breaches

The number of new *Health Information Act* files increased from 87 last year to 234 this year. The number of privacy breach notifications from health information custodians increased from 66 to 206. This is an unprecedented number of new privacy breach notices and responding to them has stretched resources thin within the OIPC. It is not yet apparent whether this situation is anomalous or whether it indicates a 'new normal'. Our office will be monitoring this workload issue over the next year.

The following custodians reported breaches this year:

- Department of Health and Social Services (DHSS);
- Hay River Health and Social Services Authority (HRHSSA);
- Tlicho Community Services Agency (Tłıchq Community Services Agency);
- Northwest Territories Health and Social Services Authority (NTHSSA)

²² <https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc28/2020ntipc28.html>

²³ 49.14. The head of a public body shall, within 120 business days of the notice given under paragraph 49.13(b), provide to the Information and Privacy Commissioner a report on the status of its implementation of recommendations accepted under section 49.13. SNWT 2019, c.8, s.34.

COVID Secretariat

Fifty-five privacy breach notifications were associated with the COVID Secretariat, a unit established within the DHSS to help manage the Northwest Territories' public health response to the pandemic. The COVID Secretariat ceased operations earlier this year, but investigations continue. Some of these breach events were significant: one instance of improperly addressed email affected over 1000 individuals. While the COVID Secretariat has disbanded, we will be completing our investigations and review of these privacy breaches. Ideally, this will assist the DHSS to avoid repeating such privacy breaches in the future.

The HIA requires unauthorized disclosures to be reported to my office and to affected individuals as soon as reasonably possible.²⁴ Most of the privacy breaches that occurred within the COVID Secretariat were not reported by DHSS in a timely manner. In some instances, months passed between the Secretariat's discovery of a privacy breach and notice to my office and the affected individuals. Investigation of these breaches has been further delayed by late final reporting and the need to seek further details regarding individual breaches and the DHSS's responses.

The number of breach notifications provided from the Covid Secretariat via DHSS, and the lack of timely and detailed reporting, has placed considerable demand on my office. Many of these matters continue as active investigations and will take some time to conclude.

NTHSSA

Most of the remaining privacy breach notices were submitted by the Northwest Territories Health and Social Services Authority (NTHSSA), which provides health services to most communities in the Northwest Territories. Breaches have frequently occurred while sending personal health information via fax and when sending emails, printing documents, and using electronic health information systems.

The increase in breach notifications does not necessarily reflect an identical increase in the number of actual breaches. Changes in operations, staffing, and training due to the pandemic likely caused some increase in actual privacy breaches. However, the increase in notifications is likely also due to better recognition and reporting of breaches. NTHSSA has taken steps to improve awareness of staff about recognizing and responding to breaches, and its reporting process is also evolving and improving. The number of notices received indicates there is more work to be done in applying the appropriate administrative, technical, and physical safeguards to protect personal health information including staff training. But, while the number of breaches is of concern, the increase in reporting also reflects positively on the custodian's efforts to satisfy obligations under the HIA, and ATIPPA.

I understand that the NTHSSA experienced a period when it lacked sufficient staff to properly document and report privacy breaches. I understand NTHSSA has addressed its need for

²⁴ See section 87, *Health Information Act*.

appropriate staffing levels and relevant training, and I expect that going forward NTHSSA will be better able to recognize, investigate, respond to, and report on breaches in a timely manner.

Recurring Issues in Privacy Breaches

Faxing

Though the circumstances may differ somewhat, the types of breaches reported are largely unchanged from previous years. While email is a significant source of privacy breaches, followed by misidentification of patients and their records, and not applying reasonable security measures to paper records, faxing remains a significant source of privacy breaches.

The incidence of unauthorized disclosure of personal health information when using fax machines has been addressed in review reports issued by this office and in past years' Annual Reports.²⁵ Faxing has also been the subject of comment by the Standing Committee on Government Operations.²⁶ GNWT has previously advised it intends to or has reduced the use of faxing related to provision of health and social services over the last decade and that it "is preparing a plan to better understand the current use of faxing across the NWT HSS system and to continue the work toward further reducing faxing."²⁷ I am not aware if this plan has yet been completed or implemented.

Despite the commitment from health information custodians and the GNWT to decrease use of fax machines, they continue to be used and mistakes continue to occur. The OIPC will continue to monitor this issue closely.

Recommendation 5: *Health information custodians should continue to reduce or eliminate the use of fax machines in connection with the provision and administration of health services across the territory.*

Vigilance required when using e-Mail

The incidence of privacy breaches involving improper use of email has been increasing. Mistaken disclosures can occur when employees send email to the wrong email address or to the wrong email group, or they attach the wrong documents to an email. Emails have been mistakenly sent to large numbers of persons who should only have received individual messages, due to using "cc" instead of the "bcc" function. Inattention to detail is often the mistake that leads to such

²⁵ For example, see 20-HIA 26 and 20-HIA 27 (CanLII) 2020 NTIPC 23 and 2020 NTIPC 24

<https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc23/2020ntipc23.html>

<https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc24/2020ntipc24.html>

²⁶ See Recommendation #3, pages 6-7 at

https://www.ntassembly.ca/sites/assembly/files/cr_30-192_-_scogo_report_on_the_review_of_the_2020-2021_annual_report_of_the_information_and_privacy_commissio.pdf

²⁷ See Government of the Northwest Territories Response to Committee Report 5-19(2): Report of the Information and Privacy Commissioner of the Northwest Territories at page 3. Located at:

https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf

privacy breaches. The use of passwords on documents and secure file transfers can help reduce the possibility of an unintended recipient being able to access someone else's personal information when using email systems.

Paper Records

Many health services are supported by electronic health information systems and communication systems. However, most locations still use paper records for some transactions. Privacy breaches have occurred when paper records have been left unsecured in plain view, or left under the glass of fax machines, or printed on printers located in wrong areas; paper records have been dropped on the ground and lost or left unsecured on desks, and paper records have been destroyed before investigators have been able to verify the extent of the information breached.

Paper records give rise to different kinds of privacy risks than electronic records, but technology can often help ameliorate risk. Technology can help by making paper records unnecessary. It can also help by limiting the possibility of unintentional disclosure through proper use of pre-programmed email addresses, password protection, limitation of available printers, etc.

Privacy Training

The Department of Health and Social Services (DHSS) created its Mandatory [Privacy] Training Policy in 2017, requiring privacy training for all employees of the Department, and the Health and Social Services Authorities. The Policy requires general and job-specific privacy training modules to be completed within three months of on-boarding new employees, and annually thereafter. It also requires the employer to keep a record of employees' training. The purpose of the Mandatory Training Policy is to ensure employees are trained to avoid or prevent privacy breaches before they occur and can respond appropriately in the event of a breach.

Lack of appropriate training and lack of documentation of training continue to be issues despite review reports issued in past years identifying these deficiencies. Custodians will often address training deficiencies as part of their response to breach events, but this should not be necessary if custodians comply with the Mandatory Training Policy. Privacy training requires the dedication of resources and requires on-going support from leadership and management to ensure annual training occurs.

Recommendation 6: *Health information custodians should prioritize implementation of and compliance with the Mandatory Training Policy and ensure that appropriate privacy training is provided for new employees, returning employees, and for all employees annually.*

Creating and maintaining a strong culture of privacy awareness and sensitivity to privacy protection issues is essential to reducing the number of privacy breaches that proceed from momentary inattention when handling personal health information.

Privacy Impact Assessments

This year our office reviewed and commented on 15 Privacy Impact Assessments (PIAs) submitted to my office by the DHSS and by the NTHSSA. Last year we reviewed and commented on seven.

The HIA requires a PIA to be done to identify potential privacy risks posed by new health care information and communication systems, or changes thereto.²⁸ It also provides the Commissioner the discretion to make comments,²⁹ presumably so the custodian can reflect on those comments when finalizing its design and implementation plans. Completing a PIA early in the planning phase of a project is better than later when other considerations (e.g., time or redesign costs) might make it difficult to add or improve privacy-protective safeguards. A PIA should be completed well before project implementation, and certainly before any personal health information is subjected to the system and used operationally.

Several of the PIAs received by my office addressed new health information management and communications systems intended to support the government's response to the COVID pandemic.³⁰ Others were unrelated to the pandemic response.³¹

Some PIAs have arrived in our office only days before the proposed project or system is scheduled to be implemented. Such timing suggests that the review and comments to the PIA from this office are viewed more as a *pro forma* exercise at the conclusion of a project rather than an integral part of an early planning and design process.

²⁸ Section 89

²⁹ Section 175

³⁰

1. Integrating use of Statistics Canada employees to do daily active monitoring to assist in the contacting of people in the NWT who may have contacted COVID-positive individuals or developed COVID symptoms. This followed on an earlier PIA addressing the use of Statistics Canada Employees for COVID Symptom Check Notification.
2. Proof of COVID Vaccination Credential to facilitate international travel
3. COVID Secretariat: Utilization of the Smartsheet application for the COVID-19 Information System.
4. The creation of a Public Health Data Repository to assist in the public health monitoring of the COVID pandemic by the Population Health Unit in the Department of Health and Social Services.
5. Addition of the AVAYA Call Centre Management system to assist in managing the GNWT's COVID response.

³¹

1. Department of Health and Social Services -- an automated wellness check in application for people engaged in an addiction recovery plan.
2. The new On-Line application process to obtain or renew Northwest Territories Health Care Cards.
3. Deployment of the BDM Pharmacy Information System in the Inuvik Regional Hospital, replacing an out-of-date system no longer supported.
4. Pilot Project of an electronic fax ("eFax") system in the Beaufort Delta region

For example, in a recent review report³² addressing the protection of confidentiality in the context of a telehealth consultation, my office requested a copy of the PIA for the Telemerge system that replaced the older telehealth system. The request was made twice in writing, but we received no response from NTHSSA. Eventually, the review proceeded on the basis that a PIA had not been completed. The review report recommended that NTHSSA conduct a PIA for the Telemerge system, a system that was replacing the older telehealth system. That recommendation was made on April 29, 2022 and accepted by NTHSSA in a letter dated May 27, 2022. That letter referred to a PIA submitted to my office on May 9, 2022. That PIA was signed by officials between February and June 2021. The PIA states that “The Telemerge migration occurred between the dates of August 13th, 2019, and February 26th, 2020.”

This approach demonstrates either a lack of commitment to, or misunderstanding of, the PIA process, and frustrates the intended operation of the HIA. My office is reviewing the Telemerge PIA, though any comments will obviously not be part of a planning exercise, as the replacement of the older Telehealth units is already underway.

While I acknowledge that PIAs are being submitted, in my view more work needs to be done to utilize the PIA as part of project design. It is essential that a PIA be completed and provided for review and comment at an early stage of project development so that any comments the Commissioner may make can be duly considered and incorporated into project design where appropriate.³³ Privacy impact assessment is not a ‘check-box’ exercise.

Lastly, the HIA requires a PIA when there is a proposed new, or a proposed change to an information system or communication technology in relation to the collection, use, or disclosure of personal health information.³⁴ The HIA does not expressly address when a PIA is to be completed or when it should be provided to the Commissioner or whether the Commissioner’s comments need be considered. Under the recent amendments to ATIPPA, a PIA is required during the development of a proposed enactment, system, project, program or service that involves the collection, use, or disclosure of personal information.³⁵ ATIPPA directs the timing of the preparation of a PIA and its submission to the Commissioner for review and comment. In my view, the wording in the ATIPPA is preferable as it requires a broader use of PIAs and explicitly directs its use as a planning tool during the development stage of a project or service.

Recommendation 7: Privacy Impact Assessments addressing any new information system or communication technology should be completed and submitted early so that there is a reasonable period for review by the Information and Privacy Commissioner and for any comment to be considered by the health information custodian in the planning stages.

³² See Northwest Territories Health and Social Services Authority (Re), 2022 NTIPC 6 (CanLII), <https://canlii.ca/t/jpfwj>

³³ This is expressed in the GNWT’s Protection of Privacy Policy 82.10. See subparagraph 6(3) at https://www.eia.gov.nt.ca/sites/eia/files/2019-09-19_protection_of_privacy_policy.pdf

³⁴ See sections 89 and 175 of HIA

³⁵ See section 42.1 of ATIPPA

Recommendation 8: *Privacy Impact Assessments should be completed for any significant change to an enactment, system, project, program, or service that involves the collection, use or disclosure of personal health information. In addition, I recommend that the Legislative Assembly consider amending section 89 of the Health Information Act to require similar use of privacy impact assessments as mandated in section 42.1 of the ATIPPA.*



Interjurisdictional Activity

Over the past year the federal, provincial, and territorial Information and Privacy Commissioners have continued to meet regularly online to share information and attend presentations about policies, technology, legislative proposals, and various other topics and issues pertaining to access to information and to privacy protection. These meetings are a valuable forum with which to stay informed of policy developments at the national and international level.

Occasionally, the Commissioners will develop a consensus decision to publish a statement or recommendation about an issue. This year the Commissioners published two joint recommendations for legislative and policy development. One addressed Reinforcing Privacy and Access to Information Rights during and After a Pandemic;³⁶ the other addressed the use of “Vaccine Passports,”³⁷ a version of which – the Personal Vaccination Certificate -- was developed for residents of the Northwest Territories.

³⁶ June 2, 2021 - Reinforcing Privacy and Access to Information Rights During and After a Pandemic : https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_210602/

³⁷ May 19, 2021 - Privacy and Covid-19 Vaccine Passports: https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210519/#fn1

Final Thoughts

Privacy protection is an ever-increasing concern as government services move increasingly online. As in some southern jurisdictions, it is now possible in the Northwest Territories to update one's health care card, get a fishing license, and register a vehicle, all online. Almost certainly, more online services will be added in the years ahead.

New technologies can offer tangible public benefits, but they can also threaten or intrude on individual privacy, and do not always consider the need to facilitate the right of access to information.³⁸ Strong policy and legal controls are required to ensure their overall beneficial use. Government adoption of new technologies must satisfy the legal requirements governing access to information and protection of privacy.

Finding the right public policy balance between access to information and protection of privacy can be challenging. When does the public interest justify an intrusion on an individual's privacy? Not everyone will share the same opinion about what personal information is necessary or appropriate to share. Disagreement about what should remain private, what is legitimately of public interest, and where the balance lies, can cause real tension, despite relevant legislation.

Our laws hold the government to certain standards and provide legal protection, both procedural and substantive, for the privacy interests we all have. An intrusion by the state into individual privacy must be carefully measured under applicable laws including the ATIPPA, the HIA, and the *Canadian Charter of Rights and Freedoms*. An intrusion on privacy must be for a reasonable purpose, demonstrably necessary and the anticipated benefit to society must be proportional to the degree of intrusion.

Laws are not static: they can and should change to ensure that laws reflect the values and needs of society. As we go forward, our office will continue to fulfill the Commissioner's obligations under the ATIPPA and HIA and to assist public bodies and health information custodians to fulfill their obligations.

³⁸ For example, collection of video recordings is increasingly common, yet there have been delays caused by public bodies' being unprepared to produce such records appropriately in response to an access to information request.

Summary of Recommendations

Recommendation 1: *The legislative assembly should consider amending the ATIPPA to allow a public body to extend the time once for the period required to complete third-party consultation without authorization by the IPC. For subsequent extensions, public bodies should continue to seek authorization from the IPC. (Page 10)*

Recommendation 2: *Public bodies that rely on the APO to discharge their ATIPPA obligations should ensure, on an ongoing basis, that the APO is staffed and resourced to a level reasonably adequate to the task. (Page 12)*

Recommendation 3: *The Legislative Assembly should consider amending the Access to Information and Protection of Privacy Act to expressly state the Information and Privacy Commissioner has discretion to extend the time required to complete a review. Such an amendment should include a requirement to give notice of an extension to all parties. (Page 13)*

Recommendation 4: *The government should consider implementing a policy, or the Legislative Assembly should consider amending the Health Information Act, to require health information custodians to report to the Commissioner regarding the implementation of accepted recommendations. (Page 14)*

Recommendation 5: *Health information custodians should continue to reduce or eliminate the use of fax machines in connection with the provision and administration of health services across the territory. (Page 16)*

Recommendation 6: *Health information custodians should prioritize implementation of and compliance with the Mandatory Training Policy and ensure that appropriate privacy training is provided for new employees, returning employees, and for all employees annually. (Page 17)*

Recommendation 7: *Privacy Impact Assessments addressing any new information system or communication technology should be completed and submitted early so that there is a reasonable period for review by the Information and Privacy Commissioner and for any comment to be considered by the health information custodian in the planning stages. (Page 19)*

Recommendation 8: *Privacy Impact Assessments should be completed for any significant change to an enactment, system, project, program, or service that involves the collection, use or disclosure of personal health information. In addition, I recommend that the Legislative Assembly consider amending section 89 of the Health Information Act to require similar use of privacy impact assessments as mandated in section 42.1 of the ATIPPA. (Page 20)*

Contact Us



**Office of the Information and Privacy Commissioner
of the Northwest Territories
PO BOX 382
Yellowknife, NT X1A 2N3**

**Phone Number: 1 (867) 669-0976
Toll Free Line: 1 (888) 521-7088
Fax Number: 1 (867) 920-2511**

Email: admin@oipc-nt.ca

Website: www.oipc-nt.ca



**Our office is located on the first floor of the Laing building in Yellowknife
Corner of Franklin Avenue & 49th Street, the entrance is on Franklin Avenue**



Territoires du Nord-Ouest

Rapport Annuel

2021 – 2022



**COMMISSARIAT À
L'INFORMATION ET
À LA PROTECTION
DE LA VIE PRIVÉE**

TERRITOIRES DU NORD-OUEST

Le 1^{er} juillet 2022

M. Frederick Blake
Président de l'Assemblée législative
C.P. 1320
Yellowknife TNO
X1A 2L9

Monsieur le Président,

Conformément à l'article 68 de la *Loi sur l'accès à l'information et la protection de la vie privée* et à l'article 173 de la *Loi sur les renseignements personnels sur la santé*, j'ai l'honneur de présenter mon rapport annuel à l'Assemblée législative des Territoires du Nord-Ouest pour la période allant du 1 avril 2021 au 31 mars 2022.

Je vous prie d'agréer, Monsieur, mes salutations distinguées.



Andrew E. Fox
Commissaire à l'information et à la protection de la vie privée
des Territoires du Nord-Ouest

/af

Table des matières

<u>Message du commissaire</u>	Page 1
<u>Rapport financier</u>	Page 3
<u>Commissariat à l'information et à la protection de la vie privée et loi habilitante</u>	Page 5
<i>Loi sur l'accès à l'information et la protection de la vie privée</i>	
<i>Loi sur les renseignements personnels sur la santé</i>	
Commissaire à l'information et à la protection de la vie privée	
<u>Bilan de l'année</u>	Page 8
Aperçu des chiffres (LAIPVP et LRS)	
<i>Loi sur l'accès à l'information et la protection de la vie privée</i>	
<i><u>Rapports d'examen</u></i>	
<i><u>Demandes de prolongation des délais</u></i>	
<i><u>Examen du projet de loi</u></i>	
<i><u>Délais prévus par la LAIPVP</u></i>	
<i>Loi sur les renseignements personnels sur la santé</i>	
<i><u>Rapports d'examen</u></i>	
<i><u>Hausse des atteintes à la vie privée</u></i>	
<i><u>Problèmes récurrents liés aux atteintes à la vie privée</u></i>	
<i><u>Évaluations des répercussions sur la vie privée</u></i>	
<u>Activités intergouvernementales</u>	Page 23
<u>Dernières réflexions</u>	Page 23
<u>Résumé des recommandations</u>	Page 24
<u>Nous joindre</u>	Page 26

Message du commissaire



Voici notre rapport annuel qui couvre la période du 1^{er} avril 2021 au 31 mars 2022 et le deuxième que nous produisons depuis que j'ai été nommé commissaire à l'information et à la protection de la vie privée le 23 novembre 2020. Cette année a été chargée! La quantité de nouveaux dossiers a connu une importante hausse par rapport à l'exercice précédent, et il semble que cette tendance soit appelée à se poursuivre. La plus forte hausse est associée aux infractions à la *Loi sur les renseignements sur la santé* (LRS), mais le Commissariat a remarqué des hausses pour pratiquement toutes les questions que nous devons traiter. Il y a donc beaucoup de travail qui attend notre nouvelle enquêteuse. Souhaitons malgré tout bienvenue à Kristen Luce Vivian!

L'un des plus importants jalons atteints durant l'exercice est probablement l'entrée en vigueur, le 30 juillet 2021, des modifications apportées à la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP). Ces modifications comprennent divers points importants :

- La prolongation des délais pour répondre à une demande d'accès à l'information exige maintenant une autorisation préalable si on compte prolonger le délai de plus de 20 jours ouvrables.
- Nous avons également éliminé certaines exceptions qui justifiaient de ne rien divulguer en réponse à certaines demandes d'accès à l'information.
- Les organismes publics doivent maintenant signaler une atteinte importante à la vie privée au Commissariat à l'information et à la protection de la vie privée, alors que les autres atteintes à la vie privée peuvent être signalées à la personne concernée si l'atteinte crée un « risque réel de préjudice grave » pour la personne.
- Les organismes publics doivent communiquer au public, à un groupe touché ou à une personne touchée toute information relative à un risque de préjudice grave pour l'environnement, ou encore pour la santé ou la sécurité du public, ou relative à toute autre raison qui est clairement dans l'intérêt du public.
- Le commissaire peut maintenant lancer un examen sans avoir reçu une plainte officielle d'un particulier.
- Il faut maintenant réaliser des évaluations des répercussions sur la vie privée dans le cadre de l'élaboration de tout système, promulgation, projet, programme ou service qui demande de collecter, de traiter ou de communiquer des renseignements personnels. Ces modifications témoignent d'une exigence de la politique établie en 2019.

Durant l'exercice, nos travaux ont été caractérisés par l'important volume de nouvelles questions à traiter. Nous avons ouvert 95 nouveaux dossiers relatifs à la LAIPVP, contre 75 à l'exercice précédent, et 234 dossiers relatifs à la LRS, une importante hausse par rapport aux 87 dossiers ouverts durant l'exercice précédent. Parmi ces dossiers, nous en comptons 50 qui touchaient des

atteintes à la vie privée liées au Secrétariat pour la COVID-19.¹ Cette hausse s'inscrit dans une tendance à long terme qui a vu les ouvertures de dossiers multipliées par 6 au CIPVP entre 2011-2012 et 2019-2020.² Cette charge accrue de dossiers à traiter nous pousse également à nous poser des questions au sujet de l'efficacité des politiques et processus de protection des renseignements personnels qui régissent les dépositaires de renseignements sur la santé et à nous préoccuper des ressources affectées aux fonctions d'accès à l'information et de protection des renseignements personnels, tant au CIPVP que pour les autres organismes publics. La hausse des nouveaux dossiers s'explique à la fois par un nombre accru d'atteintes à la vie privée et par un plus haut taux de signalement. Je prévois que la quantité de demandes d'évaluations des répercussions sur la vie privée soumises à notre Commissariat poursuivra sa hausse. Nous allons effectuer un suivi du volume et des types de nouveaux dossiers qui nous sont soumis.

Durant la pandémie, le public a bénéficié d'un meilleur accès en ligne à l'information et aux services du gouvernement. En novembre 2021, le gouvernement des Territoires du Nord-Ouest (GTNO) a élargi les services qu'il offre en ligne par l'intermédiaire de son Portail des services en ligne qui facilite les services liés aux demandes d'inscription et de renouvellement de cartes d'assurance maladie, à la production de documents d'immatriculation et de permis de conduire, à l'achat de permis de pêche, aux demandes d'aide financière aux étudiants et aux demandes d'information touchant l'apprentissage et la qualification professionnelle des métiers et professions. Le GTNO offre également en ligne un accès aux certificats de vaccination personnels dans le cadre des mesures prises par la santé publique face à la pandémie de COVID-19.

La société peut bénéficier de nouvelles façons de communiquer l'information et d'offrir des services. Les nouvelles technologies s'accompagnent toutefois de nouveaux risques. Compte tenu de la menace omniprésente de la surveillance indésirable et du vol de données, il est essentiel de faire preuve de vigilance. Alors que l'environnement en ligne change et que le gouvernement offre de plus en plus de services en ligne, nos mesures de sécurité doivent continuer d'évoluer pour protéger les renseignements personnels des menaces, nouvelles et existantes, en matière de sécurité et de protection des renseignements personnels. Les évaluations des répercussions sur la vie privée (ÉRVP) constituent un outil important qui aide le gouvernement à éviter ou à atténuer les risques. Celles-ci sont maintenant requises en vertu de la LAIPVP et de la LRS.

Les directives en matière d'isolement de la santé publique exigeaient d'effectuer du télétravail durant de longues périodes, ce qui a représenté un défi à relever en matière de gestion des dossiers. Nous avons été nombreux à travailler de notre domicile pour la première fois, et certaines personnes ont même commencé de nouveaux emplois dans ces conditions. Notre nouvelle enquêtrice a d'ailleurs commencé à collaborer avec nous plus tôt au cours de l'exercice, quand les protocoles exigeant le télétravail étaient encore en vigueur en raison de la pandémie.

¹Cette organisation est rattachée au ministère de la Santé et des Services sociaux. Certaines de ces atteintes ont eu lieu lors de l'exercice précédent, mais ont été signalées tardivement.

²On fait mention de cela dans le rapport d'examen du rapport annuel 2020-2021 du commissaire à l'information et à la protection de la vie privée produit par le Comité permanent des opérations gouvernementales (CPOG) de l'Assemblée législative. Se reporter à la page 2.

Même si nous croulions sous la charge de travail, nous avons réussi à nous adapter et à télétravailler de façon efficace pour maintenir la stabilité des services offerts au public. Les déplacements professionnels ont été évités en raison de la pandémie. Nous avons cependant été en mesure de participer à des conférences Web et de bénéficier d'autres formes d'apprentissage électronique dont le nombre a explosé, et je crois que nous continuerons d'employer une combinaison d'événements en personne et en ligne à l'avenir. Nous sommes prêts pour un autre exercice chargé.

Rapport financier

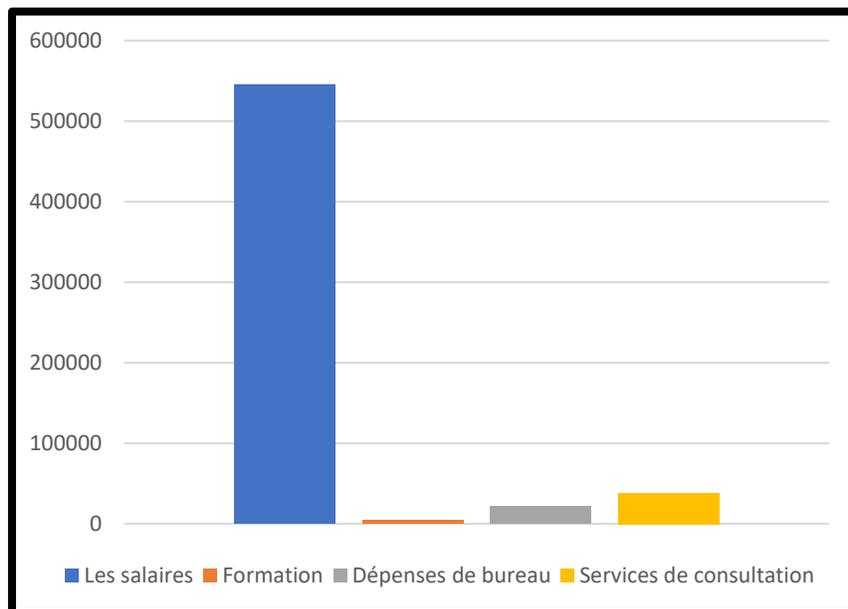
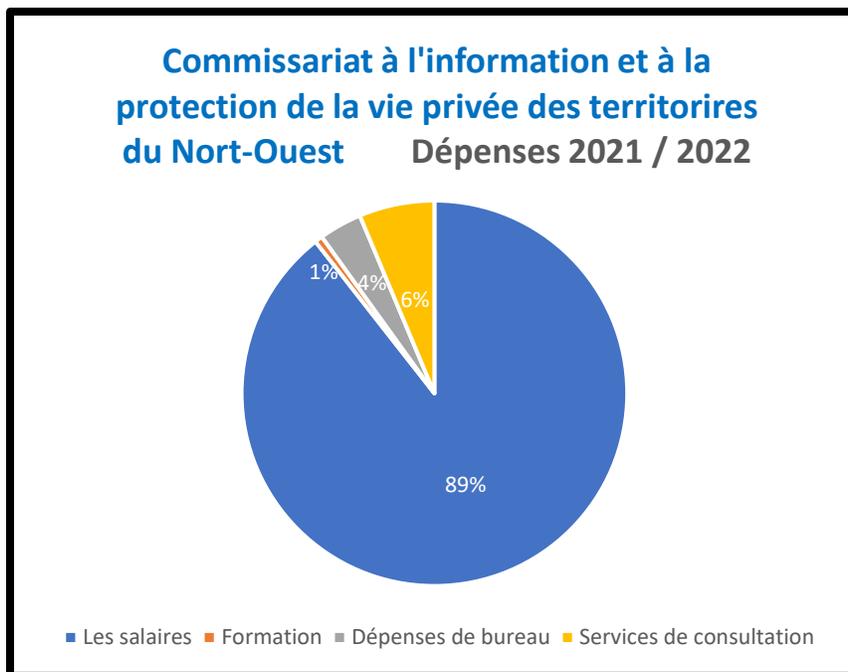
Les dépenses d'exploitation du Commissariat à l'information et à la protection de la vie privée (CIPVP) des Territoires du Nord-Ouest ont totalisé 609 279,53 \$ en 2021-2022. Vous pouvez trouver une ventilation détaillée de ces dépenses dans les tableaux de la page suivante.

Encore une fois, la gestion du budget du CIPVP n'est associée à aucune difficulté. Notre budget d'exploitation totalisait 753 000 \$, et nous avons remis un montant non dépensé de 143 720,47 \$ à l'Assemblée législative. Il existe quelques écarts entre les montants du budget et les dépenses réelles :

1. Les fonds retournés au GTNO étaient réservés à des salaires. Nos dépenses ont été inférieures aux prévisions pour diverses raisons. Tout d'abord, nous avons mis plus de temps que prévu à trouver notre enquêteuse qui est entrée en poste en janvier 2022. Ensuite, il fallait modifier les descriptions de postes actuelles, ce qui a pris plus de temps que prévu, et aussi officialiser et reprendre le processus d'évaluation au complet pour les postes de gestionnaire de bureau (devenu coordonnateur des enquêtes, des communications et des finances) et de commissaire adjoint à l'accès à l'information et la protection de la vie privée. Les répercussions de ces changements se feront sentir dans le budget 2022-2023.
2. Des coûts additionnels sont associés à la configuration des bureaux à domicile durant les périodes d'isolement. Nous ne prévoyons pas que ces coûts ponctuels se répètent.
3. Nous avons fait appel à des consultants en permanence afin d'obtenir de l'aide pour le traitement de certaines enquêtes et des ÉVRP en retard. Notre traitement des ÉVRP est maintenant à jour.
4. Nous poursuivons nos dépenses en formation et perfectionnement professionnel. Les commissaires à l'information et à la protection de la vie privée du gouvernement fédéral et des provinces et territoires ont organisé deux conférences en ligne sur le travail des enquêteurs à un prix modique. Cela constituait une merveilleuse occasion pour les plus petites organisations, comme la nôtre, d'obtenir les perspectives et les conseils d'experts des plus grandes organisations provinciales et fédérale qui ont accès non seulement à plus de ressources, mais à des ressources spécialisées. Nous prévoyons répéter lors de

chacun des exercices à venir de telles activités de perfectionnement professionnel. Une mince part de notre budget annuel continuera d'appuyer les mesures prises par les membres du personnel et de la direction pour apprendre, notamment, en obtenant accès à des documents de référence ou à une formation pertinente de nature professionnelle ou universitaire.

5. En raison des restrictions liées à la COVID-19, aucun déplacement professionnel n'a eu lieu lors de l'exercice visé par le rapport, comme c'était le cas à l'exercice précédent. Les conférences et autres possibilités d'apprentissage reviennent à la participation en personne. Par exemple, la réunion des commissaires fédéral, provinciaux et territoriaux aura lieu cette année à St. John's, Terre-Neuve-et-Labrador.



Commissariat à l'information et à la protection de la vie privée et loi habilitante

Loi sur l'accès à l'information et la protection de la vie privée

La *Loi sur l'accès à l'information et la protection de la vie privée*³(LAIPVP) s'applique à tous les ministères, bureaux et autres organes du gouvernement des Territoires du Nord-Ouest ainsi qu'à 22 agences, conseils, commissions, sociétés et autres organismes publics désignés dans les règlements de la LAIPVP.⁴ Compte tenu des modifications qui sont entrées en vigueur en 2021, les municipalités peuvent être vues comme des organismes publics aux termes de la réglementation.⁵

La LAIPVP prévoit quatre droits et obligations principaux :

- le droit du public d'avoir accès à tout document sous la garde ou le contrôle d'un organisme public, sous réserve d'exceptions limitées et particulières;
- le droit des individus d'avoir accès à leurs renseignements personnels que détiennent des organismes publics et de demander à ce que des corrections y soient apportées;
- l'obligation pour les organismes publics de protéger la vie privée des personnes en établissant les circonstances dans lesquelles ils peuvent collecter, utiliser ou divulguer des renseignements personnels;
- le droit de demander l'examen indépendant des décisions des organismes publics concernant l'accès aux dossiers gouvernementaux ou concernant la collecte, l'utilisation, la divulgation ou la correction des renseignements personnels.

La LAIPVP a deux objectifs fondamentaux : offrir au public un accès aux documents du gouvernement et protéger les renseignements personnels des particuliers en contrôlant la collecte, l'utilisation et la communication des renseignements personnels par le gouvernement. La première partie de la LAIPVP présente le droit du public d'accéder aux documents détenus par des organismes publics et le processus que doivent utiliser les membres du public pour obtenir accès à de tels dossiers. La deuxième partie précise quand et comment les organismes

³LTN-O 1994, ch. 20.

⁴Sous réserve des restrictions et exceptions figurant dans la LAIPVP ou une autre loi.

⁵À l'heure actuelle, aucune collectivité n'a encore été désignée ainsi.

publics peuvent recueillir, utiliser ou communiquer les renseignements personnels des particuliers.

Le commissaire réalise des examens indépendants des décisions et des mesures prises par les organismes publics en vertu des deux parties de la LAIPVP. Après avoir pris connaissance des faits et reçu les assertions du demandeur ou du plaignant, de l'organisme public et de toute tierce partie pertinente, le commissaire produira un rapport d'examen qui comprendra une ordonnance, et possiblement d'autres modalités. Un organisme public doit respecter une ordonnance du commissaire qui peut toutefois être portée en appel à la Cour suprême des Territoires du Nord-Ouest.

L'accès à l'information et la protection des renseignements personnels sont essentiels pour veiller à ce que le gouvernement soit transparent et responsable, ce qui est indispensable pour une démocratie saine et efficace. D'importantes modifications apportées récemment à la LAIPVP ont ajouté des exigences en matière de réaction à des atteintes à la vie privée et d'évaluation des répercussions sur la vie privée.⁶

Bien que les lois des TNO accordent un droit d'accès aux documents du gouvernement, ce droit n'est pas inconditionnel. La loi prévoit des exceptions dont l'application est soit obligatoire, soit discrétionnaire et qui permettent aux organismes publics de refuser de communiquer une partie de leurs documents. Les décisions prises à la suite d'une demande d'accès à l'information peuvent toucher à des questions complexes en ce qui a trait à établir à qui doit être communiquée l'information et à bien appliquer les exceptions prévues par la loi qui pourraient obliger ou autoriser l'organisme en question à refuser de communiquer certains renseignements. Une supervision indépendante aide le public à s'assurer que les organismes publics appliquent la LAIPVP comme il se doit. La supervision aide également les demandeurs à s'assurer que leurs droits sont bien appliqués.

Loi sur les renseignements personnels sur la santé

La *Loi sur les renseignements personnels sur la santé*⁷(LRS) régit la collecte, l'utilisation et la communication de renseignements médicaux personnels et reconnaît le droit des particuliers à accéder à leurs renseignements médicaux personnels et à les voir protégés, ainsi que la nécessité que des dépositaires collectent, utilisent et communiquent des renseignements médicaux personnels pour appuyer, gérer et offrir des soins médicaux. La LRS régit les dépositaires de renseignements médicaux dans les secteurs public et privé, ce qui comprend le ministère de la Santé et des Services sociaux, l'Administration des services de santé et des services sociaux des Territoires du Nord-Ouest, l'Administration des services de santé et des services sociaux de Hay River, l'Agence de services communautaires tįjçq ainsi que les médecins et pharmaciens des TNO qui travaillent dans le privé.

⁶D'importantes modifications ont été adoptées dans la LTN-O 2019, ch. 8 et sont entrées en vigueur le 30 juillet 2021.

⁷LTN-O 2014, ch. 2.

La LRS établit les devoirs des dépositaires de renseignements médicaux qui doivent prendre des mesures raisonnables pour protéger la confidentialité et la sécurité des renseignements médicaux des particuliers. Elle donne de plus le droit aux patients de limiter la collecte, l'utilisation et la communication de leurs renseignements médicaux personnels, et fixe des conditions précisant qui a accès aux documents médicaux personnels et à quels renseignements médicaux personnels il est possible d'obtenir accès. Les dispositions de la loi se fondent sur le principe selon lequel l'accès qu'a un prestataire de services de santé aux renseignements médicaux personnels d'un particulier devrait se limiter à l'information dont ce prestataire de services « a besoin de connaître » pour faire son travail.

La LRS exige également des dépositaires de renseignements sur la santé qu'ils avisent les personnes concernées si leurs renseignements personnels sur la santé sont utilisés ou divulgués autrement que dans les limites autorisées par la Loi ou s'ils sont volés, perdus, modifiés, ou détruits de manière inappropriée. Un avis doit être envoyé au commissaire si une communication non autorisée a lieu, ainsi qu'en cas d'utilisation, de perte ou de destruction non autorisée dans l'éventualité où il serait raisonnable de penser que le particulier en question peut subir un préjudice. Dans de telles circonstances, le commissaire peut lancer une enquête de sa propre initiative ou à la demande d'un particulier qui croit que ses renseignements médicaux ont été collectés, utilisés ou communiqués de manière à enfreindre la LRS. Après avoir réalisé un examen, le commissaire rédigera un rapport qui pourrait comprendre des recommandations à l'intention du dépositaire des renseignements médicaux. Le dépositaire doit communiquer au commissaire sa décision d'appliquer ou non les recommandations dans les 30 jours suivant la réception d'un rapport et doit appliquer toute décision de suivre les recommandations dans les 45 jours suivant la communication de son intention de se conformer aux recommandations du commissaire. Les demandeurs insatisfaits d'une décision prise par un dépositaire de renseignements médicaux relativement à une recommandation peuvent porter la décision en appel devant la Cour suprême.

Commissaire à l'information et à la protection de la vie privée

Le commissaire à l'information et à la protection de la vie privée est un agent officiel de l'Assemblée législative des Territoires du Nord-Ouest qui se voit confier par cette dernière un mandat de cinq ans. Le commissaire agit de façon indépendante du gouvernement et relève directement de l'Assemblée législative.

Les pouvoirs, devoirs et fonctions du commissaire sont précisés dans la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et dans la *Loi sur les renseignements sur la santé* (LRS). Ils sont mis en application par le Commissariat à l'information et à la protection de la vie privée (CIPVP). En plus de traiter les plaintes au sujet des réponses aux demandes d'accès à l'information et des atteintes à la vie privée, le commissaire doit également formuler des commentaires au sujet des évaluations des répercussions sur la vie privée (ÉRV) qui sont soumises au CIPVP par les organisations publiques. Les ÉRV sont généralement requises quand un organisme public ou un dépositaire de renseignements médicaux élabore un nouveau

système, projet, programme ou service qui exige de collecter, d'utiliser ou de communiquer des renseignements personnels ou des renseignements médicaux personnels. Les ÉRVP sont un outil de planification clé qui nous aide à nous assurer que nous réfléchissons, lors des étapes initiales, aux répercussions sur la protection des renseignements personnels de tout programme ou politique proposé. Une ÉRVP nous aide à confirmer si un plan s'aligne sur les exigences législatives et à relever les lacunes ou faiblesses qui devront être réglées *avant* l'étape de mise en œuvre.

Les ÉRVP sont exigées en vertu de la LRS depuis son entrée en vigueur en 2015, et elles sont maintenant exigées en vertu de la LAIPVP⁸ et de la Politique de protection de la vie privée 82.10 du GTNO.⁹ Le commissaire peut également effectuer des examens et formuler des commentaires visant les projets de loi sur le plan des répercussions possibles en matière de protection des renseignements personnels ou d'accès à l'information gouvernementale.

Bilan de l'année

Le Commissariat à l'information et à la protection de la vie privée a ouvert 329 dossiers en tout au cours de l'exercice 2021-2022. Parmi ceux-ci, 95 étaient couverts par la *Loi sur l'accès à l'information et la protection de la vie privée*, alors que les 234 autres étaient couverts par la *Loi sur les renseignements sur la santé*.

Aperçu des chiffres

Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP)

Entre le 1 avril 2021 et le 31 mars 2022, le CIPVP a ouvert 95 dossiers en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*.

Demandes d'examen – Accès à l'information et caviardage	17
Demandes d'examen – Retards et prolongations	18
Demandes d'examen — Demandes de tierces parties	9
Demandes d'examen – Problèmes de confidentialité et plaintes	18
Demande d'un organisme public - Prolongation du délai de réponse	13
Demande d'un organisme public - Demande d'accès ignorée	1
Avis d'un organisme public - Atteinte à la vie privée	13
Consultations et observations — Lois, législation, projets de loi	6

⁸Le paragraphe 42.1 est entré en vigueur le 31 juillet 2021, en même temps que les autres modifications.

⁹Cette politique est en vigueur depuis août 2019.

Loi sur les renseignements sur la santé

Entre le 1 avril 2021 et le 31 mars 2022, le CIPVP a ouvert 234 dossiers en vertu de la *Loi sur les renseignements personnels sur la santé*.

Avis d'un organisme public - Atteinte à la vie privée	206
Demande d'examen – Problèmes de confidentialité et plaintes	4
Observations — Évaluations des répercussions sur la vie privée	15
Observations — Politiques, lois et processus en matière de santé	8
Questions diverses et administratives	1

Loi sur l'accès à l'information et la protection de la vie privée

L'article 68 de la LAIPVP exige que le rapport annuel comprenne une évaluation de l'efficacité de la loi, fasse état des activités du commissaire et mentionne toutes les occasions où les recommandations figurant dans un examen n'ont pas été appliquées. Les questions suivantes touchent ces exigences, et pour certains de ces cas, j'ai recommandé à l'Assemblée législative d'y réfléchir.

Rapports d'examen

Le Commissariat a produit 27 rapports d'examen en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) en 2021-2022. Dix rapports portaient sur un examen des mesures prises par les organisations publiques en réaction à des demandes d'accès à l'information. Dix rapports portaient sur des demandes d'organisations publiques désirant une prolongation du délai accordé avant de devoir prendre des mesures en réponse à une demande d'accès à l'information. Sept rapports portaient sur un examen visant à établir si des renseignements personnels avaient été collectés, utilisés ou communiqués sans autorisation juridique.

Vous pouvez accéder aux rapports en ligne à <https://www.canlii.org/fr/nt/ntipc/>.¹⁰

Avant l'entrée en vigueur des modifications visant la LAIPVP le 30 juillet 2021, le commissaire pouvait réaliser des examens et formuler des recommandations au sujet des mesures prises par les organismes publics en réponse à des demandes d'accès à l'information et à des cas de collecte, d'utilisation, de communication ou de perte non autorisée de renseignements

¹⁰Les décisions de l'exercice précédent sont aussi disponibles en ligne sur la base de données publique gratuite.

personnels. Depuis le 30 juillet 2021, le commissaire peut produire des ordonnances à la conclusion d'un examen. Les organismes publics doivent appliquer ces ordonnances. Pour surveiller le respect des ordonnances, le Commissariat a instauré la pratique d'associer un délai à chacune des ordonnances au terme duquel l'organisme public doit faire état des mesures prises pour se plier à l'ordonnance. Cette pratique devrait aider le Commissariat à déterminer si certains problèmes touchent la mise en œuvre, ou le respect, des ordonnances. Jusqu'ici, nous n'avons relevé aucun problème de conformité.

Le commissaire peut toujours formuler des recommandations officielles à l'intention d'un organisme public en vertu de la section E de la deuxième partie de la LAIPVP. Il s'agit d'une nouvelle division qui traite des cas d'atteinte à la vie privée concernant les renseignements personnels. Si une atteinte à la vie privée est « importante », ¹¹ le ou la dirigeante de l'organisme public doit produire un rapport sur l'atteinte à la vie privée à l'intention du commissaire. Si le commissaire détermine que l'atteinte à la vie privée crée un « risque réel de préjudice grave » pour une personne ou plusieurs, il peut recommander à la dirigeante ou au dirigeant de prendre des mesures pour aviser d'autres personnes, pour limiter les conséquences de l'atteinte ou pour prévenir d'autres atteintes à la vie privée. La personne qui dirige l'organisme public devra décider d'appliquer ou non les recommandations, puis devra faire état au commissaire des recommandations acceptées et mises en œuvre. Le Commissariat n'a reçu aucun avis ou rapport lié à une atteinte à la vie privée en vertu de la section E.

Demandes de prorogation des délais

Il s'agit d'une nouvelle catégorie de rapport d'examen. Avant le 30 juillet 2021, les organismes publics pouvaient prolonger durant une « période raisonnable » le délai dont elles jouissaient pour répondre à une demande d'accès à l'information. Les prorogations étaient susceptibles d'être soumises à un examen du commissaire si la demande provenait d'un particulier. Il était peu fréquent que de telles situations mènent à la production de rapports d'examen. Le CIPVP ne participait pas au processus de suivi ou d'approbation des prorogations sauf si un demandeur communiquait avec nous pour se plaindre d'un délai déraisonnable. Si une plainte faisait état d'un retard, une enquête préliminaire du commissaire menait souvent à la résolution du problème sans qu'un examen soit nécessaire.

Depuis le 30 juillet 2021, les délais et le processus ont changé pour ce qui est de prolonger les délais. Les organismes publics disposent initialement de 20 jours ouvrables pour réagir à une demande d'accès à l'information, et elles peuvent prolonger ce délai de 20 autres jours ouvrables si elles satisfont aux conditions décrites au paragraphe 11(1). Toute prolongation supplémentaire doit être approuvée par le commissaire. Toute demande d'approbation d'une prolongation du

¹¹ Le terme n'est pas défini dans la LAIPVP, mais on peut trouver des facteurs à prendre en considération à l'alinéa 49.9(2).

délai doit être soumise avant l'échéance du délai en vigueur. Si le délai arrive à échéance avant que l'organisme public ne fournisse une réponse, il s'agit selon la loi d'un refus de répondre.¹²

Prorogation du délai en vue de consulter une tierce partie

Le Commissariat a publié 10 rapports d'examen après le 30 juillet 2021 et pour chacun de ceux-ci, on avait approuvé des prorogations permettant aux organismes publics de consulter des tierces parties avant de répondre à la demande d'accès à l'information. Le cadre de consultation de tierces parties en vertu de la LAIPVP prévoit une période de 55 jours ouvrables pour consulter une tierce partie.¹³ Cette période était dans chacun des cas supérieure à la prolongation de 20 jours ouvrables rendue possible par l'alinéa 11(1)c), et elle exige donc l'approbation du commissaire en vertu du paragraphe 11.1. Sous réserve d'une modification de la LAIPVP, nous prévoyons avoir à examiner une quantité substantielle de demandes de prorogation en vue de consultations auprès de tierces parties.

Si la LAIPVP exige que l'on consulte des tierces parties, le commissaire à l'information et à la protection de la vie privée (CIPVP) n'a aucun motif raisonnable de refuser une telle approbation. Le processus est en quelque sorte une formalité administrative qui a lieu si on doit faire appel à un consultant externe. Selon moi, il faudra réfléchir à cette situation.

Recommandation 1 : *L'Assemblée législative devrait songer à modifier la LAIPVP afin de permettre à un organisme public de prolonger une fois le délai sans l'approbation du CIPVP afin de consulter une tierce partie. Pour toute prolongation du même délai, les organismes publics devraient obtenir l'approbation du CIPVP.*

Prorogation en vue de prévenir une interférence déraisonnable avec l'exploitation d'un organisme public

L'alinéa 11(1)b) autorise une prorogation du délai de réponse si un organisme public qui a reçu une demande d'accès à l'information se voit demander une importante quantité de documents, ou s'il est nécessaire qu'il fasse des recherches pour trouver les documents demandés, ce qui perturberait de façon déraisonnable ses activités. Avant l'entrée en vigueur des modifications le 30 juillet 2021, les organismes publics faisaient souvent appel à cet alinéa afin d'obtenir une prolongation du délai de réponse à une demande d'accès à l'information, et parfois plus d'une fois. Un organisme public ne peut maintenant que s'autoriser une prorogation de 20 jours ouvrables, et doit ensuite obtenir l'approbation du commissaire pour toute autre prorogation. La question du seuil permet de tenir compte de la capacité d'un organisme public de répondre de manière raisonnable à une demande d'accès à l'information, et plus particulièrement quand une demande est exigeante à traiter pour l'organisme public.

¹²Voir le paragraphe 8(2) de la *Loi sur l'accès à l'information et la protection de la vie privée*.

¹³Cela comprend une période de 40 jours ouvrables pour rendre une décision et une période d'appel de 15 jours ouvrables.

Le gouvernement des Territoires du Nord-Ouest (GTNO) a créé le Bureau de l'accès à l'information et de la protection de la vie privée (BAIPVP) qui est chargé d'aider tous les organismes et ministères du GTNO¹⁴ à s'acquitter de leurs obligations en vertu de la LAIPVP. Grâce à ce modèle de services centralisés, le GTNO a transféré au BAIPVP un grand nombre des fonctions liées aux demandes d'accès à l'information qui relevaient des organisations publiques. Cela a pour effet de cultiver et de concentrer l'expertise au sein du Bureau et de rehausser les connaissances, l'expérience et l'efficacité qui sont essentielles au processus d'accès à l'information. Ce modèle de prestation de services nous semble bon, et le Commissariat a déjà pu remarquer les effets bénéfiques de cette initiative.

La question de la capacité demeure en suspens. Le gouvernement a récemment affirmé que « le financement initial lié à la mise en œuvre d'un bureau centralisé chargé de la LAIPVP pour le GTNO (le BAIPVP) a été versé par le ministère de la Justice pour veiller à l'uniformité à l'échelle du gouvernement du traitement des demandes d'accès à l'information en vertu de la LAIPVP et pour veiller à être doté de l'expertise et de la capacité requises pour traiter efficacement ces demandes ». ¹⁵ [traduction libre] Il s'agit là d'une déclaration d'intérêt, mais si les fonds réservés ne fournissent pas suffisamment de ressources, humaines et autres, le BAIPVP ne sera pas en mesure d'offrir le soutien adéquat pour que les organismes et ministères s'acquittent des obligations que leur impose la LAIPVP.

Bien que le BAIPVP soit le coordonnateur désigné de la réponse aux demandes d'accès à l'information¹⁶ pour les ministères et organismes du gouvernement, la production d'une réponse à une demande d'accès à l'information selon le cadre juridique demeure la responsabilité des organismes publics en question. J'ai récemment traité de cette question dans un rapport d'examen portant sur une demande de prolongation du délai en fonction de l'alinéa 11(1)b).¹⁷ On m'a indiqué que le BAIPVP souffrait d'une pénurie de personnel depuis 2 ans et que l'organisme public avait récemment échoué par 3 fois à communiquer une réponse dans le délai prévu par la loi. L'organisme public prévoyait que le BAIPVP allait accomplir les fonctions qui lui ont été attribuées alors même qu'il était évident que le BAIPVP n'était pas doté d'une capacité suffisante. Bien que chaque demande d'approbation doive être analysée séparément, il est probable qu'un organisme public soit en mesure de satisfaire aux exigences permettant d'obtenir une prolongation en vertu de l'alinéa 11(1)b) si cet organisme public doit faire faire le travail nécessaire par un autre organisme qui, de surcroît, ne dispose pas du personnel et des ressources nécessaires pour accomplir le travail. À mon avis, cette situation mérite d'être explorée davantage.

¹⁴Et la Société d'habitation des Territoires du Nord-Ouest

¹⁵Tiré du document suivant (en anglais) : [Government of the Northwest Territories Response to Committee Report 5-19\(2\): Report of the Information and Privacy Commissioner of the Northwest Territories](https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf) (page 2). Situé ici : https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf

¹⁶Depuis le 27 octobre 2020.

¹⁷Voir le document suivant (en anglais seulement) : 2022 NTIPC 10 (CanLII) <https://canlii.ca/t/jq3fd>

Recommandation 2 : *Les organismes publics qui font appel au BAIPVP pour s’acquitter de leurs obligations en vertu de la LAIPVP devraient veiller, en permanence, à ce que le BAIPVP dispose des ressources et du personnel nécessaires pour accomplir de façon raisonnable les tâches en question.*

Examens de projets de loi

En vertu de l’alinéa 67(1)c) de la LAIPVP, le commissaire à l’information et à la protection de la vie privée peut formuler des commentaires au sujet des répercussions sur la protection des renseignements personnels des projets de loi. Le Comité permanent des opérations gouvernementales a demandé deux fois au commissaire de formuler des commentaires durant l’exercice antérieur : au sujet du projet de loi 37, qui proposait quelques modifications à la LAIPVP, et au sujet du projet de loi 39, *Loi modifiant la Loi sur l’éducation postsecondaire*.

Le projet de loi 37 est entré en vigueur le 30 mars 2022, modifiant ainsi deux définitions en plus d’éliminer et de remplacer le paragraphe 49.5 de la LAIPVP. Le paragraphe 49.5 accorde au commissaire le droit de produire un rapport et des ordonnances en cas de collecte, d’utilisation ou de communication non autorisée des renseignements personnels d’un particulier.

Le projet de loi 39 a reçu la sanction de la commissaire des TNO le 31 mars 2022, ce qui a entraîné des modifications aux articles portant sur la création de comités consultatifs sur l’éducation postsecondaire. Ce projet de loi proposait un certain nombre de modifications à la *Loi sur l’éducation postsecondaire* qui a été promulguée par la 18^e Assemblée législative en 2019, mais qui n’est pas encore entrée en vigueur. J’ai formulé des commentaires au sujet de la création de comités consultatifs sur l’éducation postsecondaire et de la question d’établir si les documents issus de tels comités peuvent faire l’objet de demandes de production en vertu de la LAIPVP, ou si on prévoit les assujettir à une exemption.

Délais prévus par la LAIPVP

Avant l’entrée en vigueur des modifications à la LAIPVP le 30 juillet 2021, la loi prévoyait qu’un examen devait être réalisé dans les 180 jours suivant la réception d’une demande d’examen.¹⁸ Cette période a été réduite et est maintenant de 90 jours ouvrables.

Bien que le CIPVP appuie l’objectif d’offrir un processus d’examen rapide, le respect d’un délai réduit est difficile à réaliser dans la pratique. La durée moyenne d’un examen à ce moment était légèrement supérieure à 12 mois, ce qui est nettement supérieur à 180 jours. Nous avons accueilli notre nouvelle enquêtrice en janvier 2022 et son aide nous sera certainement salutaire. Son poste a toutefois été approuvé en 2020 en se fondant sur l’augmentation de la charge de travail remarquée au cours des années précédentes. Bien que le personnel du CIPVP soit

¹⁸Voir le paragraphe 31(3).

maintenant passé de trois à quatre membres (y compris le commissaire), le nombre de dossiers portés à l'attention du Commissariat a doublé durant la même période.

Bien que le Commissariat continue de travailler de manière aussi efficace et exhaustive que possible, il est peu probable que la plupart des examens seront effectués en 90 jours ouvrables. Je présume que je ne perdrai pas mon pouvoir de compétence si je mets plus de 90 jours à effectuer un examen. En essayant de respecter ce délai à tout prix, j'irais fondamentalement à l'encontre des objectifs de la LAIPVP et de la capacité du public à demander un examen à titre de recours. Bien qu'il puisse être utile d'inscrire un délai « de référence » dans la LAIPVP en matière de réalisation des examens, il serait bénéfique de clarifier le processus d'examen en inscrivant clairement que le commissaire est en mesure de prolonger le délai de réalisation d'un examen.

Recommandation 3 : *L'Assemblée législative devrait songer à modifier la Loi sur l'accès à l'information et la protection de la vie privée en y inscrivant expressément que le commissaire à l'information et à la protection de la vie privée jouit du pouvoir discrétionnaire de prolonger le délai accordé pour réaliser un examen. Une telle modification comprendrait l'exigence d'aviser toutes les parties quand une telle prorogation est accordée.*

Loi sur les renseignements personnels sur la santé

Rapports d'examen

Durant la période visée par le rapport, le Commissariat a publié trois rapports d'examen en vertu de la *Loi sur les renseignements sur la santé*. Ces rapports, comme ceux publiés en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*, sont disponibles en ligne à l'adresse <https://www.canlii.org/fr/nt/ntipc/>.

Le paragraphe 173(b) de la *Loi sur les renseignements sur la santé* exige la production d'un rapport annuel faisant état des recommandations faites dans les rapports destinés aux dépositaires des renseignements médicaux personnels qui n'ont pas été acceptées. Durant l'exercice, toutes les recommandations produites ont été acceptées par les dépositaires des renseignements médicaux personnels, ce qui indique que les recommandations seront suivies.

Solutions de rechange

La baisse du nombre de rapports indique entre autres une hausse des solutions de rechange employées pour résoudre de telles questions. Les examens menant à la production de rapports qui comprennent des recommandations à l'intention des dépositaires¹⁹ ne représentent qu'un des processus possibles. On peut également travailler avec le dépositaire des renseignements médicaux personnels pour traiter une question par l'intermédiaire d'un processus de règlement des différends²⁰, ou d'une façon encore moins officielle, en formulant tout simplement des commentaires et des orientations permettant de déceler les ressources auxquelles il faudra réfléchir. Cette approche souple continue d'engendrer de bonnes réactions chez les dépositaires et a poussé ces derniers à élaborer de nouvelles mesures de

¹⁹À la demande d'une personne en vertu de l'article 134 ou à l'initiative du commissaire en vertu de l'article 137.

²⁰ Article 138

prévention des atteintes à la vie privée et des mesures supérieures de réaction à de telles atteintes. Je vais continuer à employer cette approche le cas échéant.

Répondre aux recommandations du commissaire

Une fois un examen terminé, le commissaire produit un rapport qui pourrait contenir des recommandations. Après avoir reçu un rapport d'examen, un dépositaire dispose de 30 jours pour décider d'accepter une recommandation et aviser le commissaire de sa décision.²¹ Selon la LRS, une omission d'aviser la commissaire de sa décision dans les 30 jours sera interprétée comme une décision de ne pas suivre les recommandations du commissaire.

Malgré cette disposition d'interprétation, les réponses aux recommandations du commissaire sont souvent en retard. Prenons un exemple récent²² où le commissaire a produit un rapport d'examen (en anglais seulement) comprenant 8 recommandations à l'intention du dépositaire en mai 2020. Le dépositaire n'a pas fourni de réponse digne de ce nom avant le 30 juin 2021. Des lettres de rappel ont été envoyées au dépositaire qui a d'ailleurs reconnu la nécessité de produire une réponse en septembre 2020. Après 9 mois supplémentaires, le dépositaire a accepté l'ensemble des recommandations. Le retard a été justifié par les défis opérationnels découlant de la pandémie. À l'avenir, nous espérons voir un meilleur respect de l'exigence juridique de répondre aux recommandations dans les 30 jours.

Une fois une recommandation acceptée, la LRS exige du dépositaire qu'il applique la recommandation dans les 45 jours suivant cette décision. La LRS ne prévoit toutefois aucun mécanisme de surveillance de la mise en œuvre d'une recommandation approuvée par un dépositaire. Le Commissariat ne dispose pas du pouvoir ou des ressources nécessaires pour mener ce type de surveillance, et de plus, aucune disposition juridique n'oblige les dépositaires des renseignements à communiquer de l'information sur la mise en œuvre des recommandations acceptées. Par comparaison, le paragraphe 49.14 de la nouvelle version de la LAIPVP crée une telle obligation.²³ À mon avis, il serait utile d'avoir un processus officiel de communication d'information relative à la mise en œuvre des recommandations.

Recommandation 4 : Le gouvernement devrait réfléchir à mettre en œuvre une politique, ou l'Assemblée législative devrait réfléchir à modifier la Loi sur les renseignements sur la santé, de façon à exiger des dépositaires de renseignements médicaux d'informer le commissaire de la mise en œuvre des recommandations acceptées.

²¹Article 156

²²<https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc28/2020ntipc28.html>

²³49.14. Le responsable d'un organisme public fournit au commissaire à l'information et à la protection de la vie privée, dans les 120 jours ouvrables de la transmission de l'avis en vertu de l'alinéa 49.13b), un rapport de l'état de la mise en œuvre des recommandations acceptées en vertu de l'article 49.13. LTN-O 2019, ch. 8, art. 34.

Accroissement des atteintes à la vie privée

Par rapport à l'exercice précédent, la quantité de dossiers traités en vertu de la *Loi sur les renseignements sur la santé* est passée de 87 à 234. Le nombre d'avis d'atteintes à la vie privée issus de dépositaires de renseignements médicaux est pour sa part passé de 66 à 206. Il s'agit là d'un nombre jamais vu d'avis d'atteintes à la vie privée, et le traitement de ces avis a été extrêmement exigeant pour les ressources du CIPVP. Nous ne pouvons pas pour l'instant établir s'il s'agit d'une hausse anormale ou si c'est devenu la norme. Le Commissariat surveillera de près la question de la charge de travail durant le prochain exercice.

Les dépositaires ci-dessous ont signalé des atteintes durant l'exercice :

- Ministère de la Santé et des Services sociaux (MSSS)
- Administration des services de santé et des services sociaux de Hay River
- Agence de services communautaires t̄jchq̄
- Administration des services de santé et des services sociaux des Territoires du Nord-Ouest

Secrétariat pour la COVID-19

55 avis d'atteinte à la vie privée sont associés au Secrétariat pour la COVID-19, un service créé au sein du MSSS pour appuyer la gestion de la pandémie par les services de santé publique des Territoires du Nord-Ouest. Le Secrétariat pour la COVID-19 a mis fin à ses activités plus tôt au cours de l'exercice, mais les enquêtes se poursuivent. Certaines de ces atteintes ont eu des répercussions importantes : dans un des cas, un courriel envoyé à la mauvaise adresse a touché plus de 1 000 personnes. Bien que le Secrétariat pour la COVID-19 n'existe plus, nous allons terminer nos enquêtes et examens visant ces atteintes à la vie privée. Idéalement, cela aidera le MSSS à éviter que de telles atteintes à la vie privée se reproduisent.

La LRS exige que les divulgations non autorisées soient signalées au Commissariat et aux personnes touchées dès que raisonnablement possible.²⁴ La plupart des atteintes à la vie privée concernant le Secrétariat pour la COVID-19 n'ont pas été signalées en temps voulu par le MSSS. Dans certains cas, des mois se sont écoulés après la découverte d'une atteinte, avant que le Secrétariat ne la communique au Commissariat et aux personnes touchées. Les enquêtes sur ces atteintes ont également été retardées par une production en retard du rapport final et par le besoin de trouver d'autres renseignements liés aux atteintes elles-mêmes et à la réaction du MSSS.

Le nombre d'avis d'atteinte à la vie privée transmis par le Secrétariat pour la COVID-19 par l'intermédiaire du MSSS, et les rapports soumis en retard et ne comprenant pas l'information nécessaire, ont représenté un défi très difficile à surmonter pour le Commissariat. Il demeure des enquêtes à conclure, ce qui exigera un certain temps.

²⁴Voir l'article 87 de la *Loi sur les renseignements sur la santé*.

ASTNO

La plupart des avis d'atteinte à la vie privée qui restent à traiter ont été soumis par l'Administration des services de santé et des services sociaux des Territoires du Nord-Ouest (ASTNO), un organisme qui offre des services de santé à la majorité des collectivités des Territoires du Nord-Ouest. Les atteintes ont souvent eu lieu alors qu'on transmettait des renseignements médicaux personnels par télécopieur ou par courriel, lorsqu'on imprimait des documents et lorsqu'on utilisait les systèmes informatiques contenant les renseignements médicaux.

Cette hausse des avis d'atteinte à la vie privée ne doit pas automatiquement être interprétée comme une hausse du nombre réel d'atteintes. Les modifications apportées aux procédures, au personnel et à la formation ont probablement causé une part de la hausse des atteintes réelles à la vie privée. En revanche, la hausse du nombre d'avis s'explique probablement aussi par des améliorations du côté de la reconnaissance et du signalement des atteintes. L'ASTNO a pris des mesures pour sensibiliser davantage les membres du personnel, de façon à ce qu'ils soient plus aptes à reconnaître les atteintes et à y réagir, et le processus de signalement est en cours d'amélioration. Le nombre d'avis reçus indique qu'il y a plus de travail à faire du côté de l'application des mesures de prévention appropriées sur les plans administratif, technique et physique afin de protéger les renseignements médicaux personnels, notamment en matière de formation des membres du personnel. Bien que le nombre d'atteintes soit inquiétant, la hausse des signalements indique aussi les efforts déployés par le dépositaire de l'information pour satisfaire à ses obligations en vertu de la LRS et de la LAIPVP.

Je comprends que l'ASTNO vient de vivre une période durant laquelle elle ne disposait pas de suffisamment d'employés pour documenter les atteintes à la vie privée et y réagir comme il se doit. Je comprends aussi que l'ASTNO a résolu ses problèmes de dotation et de formation, et je m'attends donc à ce que l'organisme soit mieux à même de reconnaître les atteintes, d'y réagir, de faire enquête et de les signaler en temps opportun.

Problèmes récurrents liés aux atteintes à la vie privée

Télécopies

Bien que les circonstances puissent être légèrement différentes, les types d'atteintes signalées pour l'exercice sont globalement les mêmes que pour les exercices précédents. Bien que le courriel soit une importante source d'atteintes à la vie privée, suivie par les problèmes d'identification de patients ou de dossiers et par l'application de mesures de sécurité insuffisantes aux dossiers imprimés, les communications par télécopieur demeurent une importante source d'atteintes.

L'incidence de la divulgation non autorisée de renseignements médicaux personnels à l'aide de télécopieurs a été traitée dans des rapports d'examen produits par le Commissariat ainsi que

dans les rapports annuels des exercices précédents.²⁵ Les envois par télécopieur ont également fait l'objet de commentaires du Comité permanent des opérations gouvernementales.²⁶ Le GTNO a indiqué qu'il a déjà réduit l'utilisation des télécopies durant la dernière décennie et qu'il souhaite la réduire davantage pour offrir des services de santé et des services sociaux; le gouvernement a indiqué être en train d'élaborer un plan qui nous permettra de mieux comprendre l'utilisation qu'on fait des télécopieurs à l'heure actuelle dans le système de la santé et des services sociaux des TNO et continuer de déployer des efforts pour réduire encore l'utilisation des télécopieurs.²⁷ Je ne sais pas si ce plan a été publié ou mis en œuvre.

Malgré les engagements pris par les dépositaires de renseignements médicaux personnels et l'utilisation réduite des télécopieurs par le GTNO, on continue de les utiliser et de commettre des erreurs. La Commissariat continuera de surveiller cette question de près.

Recommandation 5 : *Les dépositaires des renseignements médicaux personnels devraient continuer à réduire ou à éliminer l'utilisation de télécopieurs pour offrir et administrer des services de santé dans l'ensemble de notre territoire.*

Il faut faire preuve de vigilance quand on envoie des courriels

L'incidence des atteintes à la vie privée associées à une utilisation erronée des courriels est en hausse. Les divulgations erronées peuvent avoir lieu quand les employés envoient des courriels à la mauvaise adresse électronique ou à un mauvais groupe de destinataires, ou quand ils associent la mauvaise pièce jointe à un courriel. Des courriels ont été envoyés à d'importants groupes de personnes qui n'auraient dû recevoir que des messages individuels en raison d'une confusion entre les fonctions « CC » et « CCI ». Les lacunes liées au souci du détail sont souvent les erreurs qui mènent à de telles atteintes à la vie privée. L'emploi de mots de passe pour les documents et du transfert de fichiers sécurisé peut contribuer à réduire le risque qu'un destinataire imprévu obtienne accès aux renseignements personnels d'une autre personne quand on utilise le courrier électronique.

Dossiers imprimés

De nombreux services de santé sont appuyés par des systèmes de communication et des systèmes électroniques de renseignements médicaux. La plupart des établissements utilisent toutefois encore des dossiers imprimés pour certaines opérations. Des atteintes à la vie privée ont eu lieu quand des dossiers imprimés ont été laissés sans surveillance et à la vue de tous, sous

²⁵Vous pouvez par exemple consulter les documents suivants (en anglais seulement) : 20-HIA 26 et 20-HIA 27 (CanLII) 2020 NTIPC 23 et 2020 NTIPC 24

<https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc23/2020ntipc23.html>

<https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc24/2020ntipc24.html>

²⁶Voir la recommandation n° 3 aux pages 6 et 7 (en anglais seulement) :

https://www.ntassembly.ca/sites/assembly/files/cr_30-192_-_scogo_report_on_the_review_of_the_2020-2021_annual_report_of_the_information_and_privacy_commissio.pdf

²⁷Tiré du document suivant (en anglais) : Government of the Northwest Territories Response to Committee Report 5-19(2): Report of the Information and Privacy Commissioner of the Northwest Territories (page 3). Situé ici :

https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf

la vitre d'un télécopieur, ou encore imprimés au mauvais endroit. Des dossiers imprimés ont été échappés au sol, ou encore perdus, ou laissés sur un bureau sans protection, et d'autres ont même été détruits avant qu'un enquêteur ait pu confirmer l'ampleur des renseignements touchés par l'atteinte.

Les dossiers imprimés donnent lieu à différents risques pour les renseignements personnels que les dossiers électroniques, mais la technologie contribue souvent à réduire les risques. La technologie peut contribuer à rendre inutiles les dossiers imprimés. Elle peut aussi réduire le risque de divulgation non intentionnelle, grâce aux adresses de courriel préprogrammées, aux mots de passe, aux restrictions des imprimantes accessibles, etc.

Formation sur la protection des renseignements personnels

Le ministère de la Santé et des Services sociaux (MSSS) a créé en 2017 une politique sur la formation obligatoire en matière de protection des renseignements personnels qui doit être suivie par tous les employés du ministère et des administrations des services de santé et des services sociaux. Cette politique exige de suivre des modules de formation généraux et propres à un emploi dans les trois mois suivant l'intégration d'un employé, et une fois par année par la suite. La politique exige également que l'employeur tienne un dossier de la formation donnée aux employés. La politique sur la formation obligatoire nous sert à veiller à ce que les employés soient formés à éviter ou à prévenir les atteintes à la vie privée, ou à y réagir comme il se doit.

L'absence de formation et de documentation des activités de formation sont des problèmes qui demeurent, malgré la publication de rapports d'examen qui soulignent ces lacunes durant les dernières années. Les dépositaires de l'information corrigent souvent les défaillances dans le cadre de leur réaction à une atteinte à la vie privée, ce qui ne serait pas nécessaire s'ils avaient respecté la politique sur la formation obligatoire. La formation sur la protection des renseignements personnels exige des ressources et un soutien permanent de la part des directeurs et des gestionnaires si on veut que les employés suivent la formation annuelle.

Recommandation 6 : *Les dépositaires des renseignements médicaux personnels devraient accorder la priorité à la mise en œuvre et au respect de la politique sur la formation obligatoire et veiller à ce que la formation nécessaire en matière de protection des renseignements personnels soit donnée aux nouveaux employés, aux employés qui font un retour au travail, et à tous les employés sur une base annuelle.*

Il est essentiel de créer et de maintenir une culture de sensibilisation à la protection des renseignements personnels et de connaissance des problèmes connexes pour réduire la quantité d'atteintes à la vie privée attribuables à un moment d'inattention lors du traitement de renseignements personnels.

Évaluations des répercussions sur la vie privée

Au cours de l'exercice, le Commissariat a reçu, de la part du MSSS et de l'ASTNO, 15 évaluations des répercussions sur la vie privée (ÉRVP), pour ensuite formuler des commentaires. Lors de l'exercice précédent, nous avons consulté 7 ÉRVP et produit des commentaires connexes.

La LRS exige que l'on réalise une ÉRVP pour désigner les risques pour les renseignements personnels posés par les nouveaux systèmes informatiques et de communication associés aux soins de santé et les changements qu'on y apporte.²⁸ Elle confère de plus au commissaire le pouvoir discrétionnaire de formuler des commentaires,²⁹ afin que le dépositaire des renseignements puisse tenir compte de ces commentaires avant d'officialiser ses plans de conception et de mise en œuvre. Il est préférable d'effectuer une ÉRVP tôt durant la phase de planification que plus tard, quand d'autres considérations (temps ou coûts associés à une reprise de la conception) peuvent compliquer l'ajout ou l'amélioration de mesures de protection des renseignements personnels. Il faut effectuer une ÉRVP bien avant la mise en œuvre d'un projet, et sans aucun doute avant que tout renseignement médical personnel soit chargé dans le système ou utilisé dans un environnement opérationnel.

Plusieurs des ÉRVP transmises au Commissariat touchaient de nouveaux systèmes de gestion et de communication de renseignements médicaux censés appuyer la réaction du gouvernement à la pandémie de COVID-19.³⁰ Bien sûr, d'autres n'étaient pas liées la réaction à la pandémie.³¹

²⁸Article 89

²⁹Article 175

³⁰

1. Intégration d'employés de Statistique Canada qui effectuent une surveillance quotidienne afin de nous aider à communiquer avec les habitants des TNO qui pourraient avoir présenté des symptômes de COVID-19 ou avoir été en contact avec des personnes ayant eu un résultat positif pour la COVID-19. Cela suivant une ÉRVP qui portait sur l'utilisation d'employés de Statistique Canada pour les avis de vérification des symptômes de la COVID-19.
2. Preuve de vaccination contre la COVID-19 visant à faciliter les déplacements internationaux.
3. Secrétariat pour la COVID-19 : utilisation de l'application Smartsheet pour les systèmes informatiques liés à la COVID-19.
4. La création d'un registre de données de la santé publique pour aider la santé publique, et plus particulièrement la Division de la santé de la population du ministère de la Santé et des Services sociaux, à effectuer une surveillance de la pandémie de COVID-19.
5. Ajout du système de gestion de centres d'appels AVAYA pour nous aider à gérer la réaction du GTNO à la pandémie de COVID-19.

³¹

1. Ministère de la Santé et des Services sociaux : une application automatisée de vérification du mieux-être des personnes qui participent à un plan de lutte contre les dépendances.
2. Le nouveau processus de demande en ligne pour obtenir ou renouveler une carte d'assurance maladie des TNO.
3. Déploiement du système d'information sur les pharmacies BDM à l'Hôpital régional d'Inuvik pour remplacer un système désuet qui n'était plus pris en charge.
4. Projet pilote d'un système de télécopie électronique dans la région de Beaufort-Delta.

Certaines des ÉRVP parviennent au Commissariat quelques jours seulement avant la date prévue de mise en service du projet ou système en question. Avec de tels délais, nous pouvons remarquer que les examens et les commentaires sur les ÉRVP formulés par le Commissariat sont vus comme un exercice *pro forma* qui a lieu à la conclusion d'un projet, plutôt que comme une partie intégrante de la planification et de la conception.

Par exemple, dans le cadre de la production d'un rapport d'examen³² touchant la protection de la confidentialité lors d'une consultation par le service de télésanté, le Commissariat a demandé une copie de l'ÉRVP visant le système Telemerge qui a remplacé l'ancien système de télésanté. Nous avons communiqué la demande par écrit à deux reprises sans obtenir de réponse de l'ASTNO. En fin de compte, nous avons dû effectuer l'examen sans compter sur une ÉRVP remplie. Le rapport d'examen recommandait à l'ASTNO d'effectuer une ÉRVP pour le système Telemerge. La recommandation a été faite le 29 avril 2022 et acceptée par l'ASTNO dans une lettre datée du 27 mai 2022. Cette lettre faisait référence à une ÉRVP soumise au Commissariat le 9 mai 2022. L'ÉRVP a été signée par les responsables entre février et juin 2021. Selon le document, la « migration vers Telemerge a eu lieu entre le 13 août 2019 et le 26 février 2020 » [traduction libre].

Cette approche démontre soit un faible engagement soit une mauvaise compréhension du processus d'ÉRVP, et elle va à l'encontre de l'application prévue de la LRS. Le Commissariat est en train de réaliser un examen de l'ÉRVP visant Telemerge, mais il est évident qu'on ne tiendra pas compte de mes commentaires dans le cadre de la planification, car le remplacement de l'ancien système de télésanté est déjà commencé.

Je reconnais qu'on nous a soumis des ÉRVP, mais selon moi, il faudra déployer plus d'efforts pour que les ÉRVP soient utiles dans le cadre de la conception d'un projet. Il est essentiel de soumettre une ÉRVP pour que je puisse réaliser un examen et formuler des commentaires au début de l'élaboration d'un projet et afin que mes commentaires puissent être pris en considération et incorporés à la conception du projet s'ils sont convenables.³³ L'évaluation des répercussions sur la vie privée représente plus qu'une case à cocher.

En dernier lieu, la LRS exige une ÉRVP si on propose un nouveau système ou une modification à un système informatique ou de communication lié à la collecte, à l'utilisation ou à la transmission de renseignements médicaux personnels.³⁴ La LRS ne précise pas hors de tout doute dans quelle situation il faut remplir une ÉRVP et la soumettre au commissaire, ou s'il est nécessaire de tenir compte des commentaires du commissaire. Compte tenu des modifications apportées récemment à la LAIPVP, il faut produire une ÉRVP durant l'élaboration de tout système, promulgation, projet, programme ou service qui nécessite de collecter, de traiter ou de

³²Voir le document (en anglais seulement) intitulé Northwest Territories Health and Social Services Authority (Re), 2022 NTIPC 6 (CanLII), <https://canlii.ca/t/jpfwj>

³³Cela est exprimé dans la politique de protection de la vie privée du GTNO 82.10. Voir le paragraphe 6(3) à https://www.eia.gov.nt.ca/sites/eia/files/82.10_politique_sur_la_protection_de_la_vie_privee.pdf

³⁴Voir les articles 89 et 175 de la LRS.

communiquer des renseignements personnels.³⁵ La LAIPVP précise à quel moment il faut produire l'ÉRVP et la soumettre au commissaire afin que ce dernier puisse effectuer l'examen et formuler des commentaires. Selon moi, le texte de la LAIPVP est préférable, car il exige une utilisation plus large des ÉRVP et précise la nécessité de les utiliser comme outil de planification durant la phase d'élaboration d'un projet ou d'un service.

Recommandation 7 : *Il faut remplir et soumettre rapidement une évaluation des répercussions sur la vie privée pour tout nouveau système d'information ou technologie de communication afin de donner un délai raisonnable pour un examen réalisé par le commissaire à l'information et à la protection de la vie privée, et afin que le dépositaire des renseignements médicaux dispose du temps nécessaire pour tenir compte des commentaires du commissaire lors des étapes de planification.*

Recommandation 8 : *Il faut remplir une évaluation des répercussions sur la vie privée chaque fois qu'une modification importante est apportée à une promulgation, un système, un projet, un programme ou un service qui demande de collecter, d'utiliser ou de communiquer des renseignements médicaux personnels. Je recommande également que l'Assemblée législative songe à modifier l'article 89 de la Loi sur l'information sur la santé afin d'exiger une utilisation des évaluations des répercussions sur la vie privée semblable à celle qui est rendue obligatoire au paragraphe 42.1 de la LAIPVP.*



³⁵Voir le paragraphe 42.1 de la LAIPVP.

Activités intergouvernementales

Durant la dernière année, les commissaires à l'information et à la protection de la vie privée du gouvernement fédéral et des provinces et territoires ont poursuivi leurs rencontres régulières en ligne en vue de communiquer de l'information et de participer à des présentations au sujet des politiques, de la technologie, des projets de loi et de divers autres sujets et questions liées à l'information et à la protection des renseignements personnels. Ces réunions ont été d'une aide précieuse en ce qui a trait à rester au courant des développements de la politique nationale et internationale.

À l'occasion, les commissaires arrivent à un consensus et publient une déclaration ou des recommandations au sujet d'une question précise. Lors de l'exercice, les commissaires ont publié conjointement deux recommandations visant l'élaboration des lois et des politiques. Dans l'une, on traite du renforcement du droit d'accès à l'information et du droit à la vie privée après une pandémie;³⁶ dans l'autre, on traite de l'utilisation de passeports vaccinaux³⁷, dont une version, le certificat de vaccination personnel, a été créée pour les résidents des Territoires du Nord-Ouest.

Dernières réflexions

Alors que les gouvernements offrent de plus en plus de services en ligne, la protection des renseignements personnels devient de plus en plus préoccupante. Comme c'est le cas dans certaines administrations du Sud, il est maintenant possible de mettre à jour sa carte d'assurance maladie, d'obtenir un permis de pêche ou d'immatriculer un véhicule en ligne aux Territoires du Nord-Ouest. Il est quasiment certain que des services en ligne supplémentaires seront offerts durant les prochaines années.

Les nouvelles technologies peuvent offrir des avantages réels aux membres du public, mais elles peuvent aussi menacer la protection des renseignements personnels, et elles ne tiennent pas toujours compte du besoin de faciliter l'accès à l'information.³⁸ Nous aurons besoin de politiques et de mesures de contrôle juridiques solides pour veiller à ce que l'utilisation des nouvelles technologies soit globalement avantageuse. L'adoption de nouvelles technologies par le

³⁶2 juin 2021 – Renforcer le droit à la vie privée et à l'accès à l'information pendant et après une pandémie : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_210602/

³⁷19 mai 2021 – La vie privée et les passeports vaccinaux relatifs à la COVID-19 : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2021/s-d_20210519/

³⁸Par exemple, on collecte de plus en plus d'enregistrements vidéo, mais certains retards ont lieu puisque des organismes publics n'étaient pas prêts à produire de tels documents de façon convenable en réaction à une demande d'accès à l'information.

gouvernement doit satisfaire aux exigences juridiques qui régissent l'accès à l'information et la protection des renseignements personnels.

Il peut être difficile de trouver un juste équilibre dans les politiques publiques entre l'accès à l'information et la protection des renseignements personnels. Quand l'intérêt du public justifie-t-il une violation du droit à la vie privée d'une personne? Les avis divergent sur les renseignements personnels qu'il faut, ou que nous devrions, communiquer. Il existe différentes opinions au sujet de ce qui doit rester dans la sphère privée ou de ce qui relève légitimement de l'intérêt du public; il est difficile de trouver un équilibre, et le sujet peut engendrer des tensions malgré l'existence de lois en la matière.

Nos lois imposent certaines normes à nos gouvernements et offrent une mesure de protection juridique (droit procédural et droit substantiel) pour nos intérêts communs en matière de protection des renseignements personnels. Une intrusion de l'État dans la sphère privée d'un particulier doit être soigneusement analysée en fonction des lois applicables, notamment la LAIPVP, la LRS et la *Charte canadienne des droits et libertés*. Une violation du droit à la vie privée doit avoir lieu pour une raison précise, et on doit pouvoir démontrer sa nécessité et ses avantages pour la société, qui doivent être proportionnels à l'ampleur de la violation.

Les lois ne sont pas éternelles : elles peuvent et elles doivent changer pour nous assurer qu'elles témoignent des valeurs et des besoins de notre société. À l'avenir, le Commissariat continuera de s'acquitter des obligations du commissaire en vertu de la LAIPVP et de la LRS et d'aider les organismes publics et les dépositaires de renseignements médicaux personnels à s'acquitter de leurs obligations.

Résumé des recommandations

Recommandation 1 : *L'Assemblée législative devrait songer à modifier la LAIPVP afin de permettre à un organisme public de prolonger une fois le délai sans l'approbation du CIPVP afin de consulter une tierce partie. Pour toute prolongation du même délai, les organismes publics devraient obtenir l'approbation du CIPVP. Page 11*

Recommandation 2 : *Les organismes publics qui font appel au BAIPVP pour s'acquitter de leurs obligations en vertu de la LAIPVP devraient veiller, en permanence, à ce que le BAIPVP dispose des ressources et du personnel nécessaires pour accomplir de façon raisonnable les tâches en question. Page 13*

Recommandation 3 : *L'Assemblée législative devrait songer à modifier la Loi sur l'accès à l'information et la protection de la vie privée en y inscrivant expressément que le commissaire à l'information et à la protection de la vie privée jouit du pouvoir discrétionnaire de prolonger le délai accordé pour réaliser un examen. Une telle modification comprendrait l'exigence d'aviser toutes les parties quand une telle prorogation est accordée. Page 14*

Recommandation 4 : *Le gouvernement devrait réfléchir à mettre en œuvre une politique, ou l'Assemblée législative devrait réfléchir à modifier la Loi sur les renseignements sur la santé, de façon à exiger des dépositaires de renseignements médicaux d'informer le commissaire de la mise en œuvre des recommandations acceptées. Page 15*

Recommandation 5 : *Les dépositaires des renseignements médicaux personnels devraient continuer à réduire ou à éliminer l'utilisation de télécopieurs pour offrir et administrer des services de santé dans l'ensemble de notre territoire. Page 18*

Recommandation 6 : *Les dépositaires des renseignements médicaux personnels devraient accorder la priorité à la mise en œuvre et au respect de la politique sur la formation obligatoire et veiller à ce que la formation nécessaire en matière de protection des renseignements personnels soit donnée aux nouveaux employés, aux employés qui font un retour au travail, et à tous les employés sur une base annuelle. Page 19*

Recommandation 7 : *Il faut remplir et soumettre rapidement une évaluation des répercussions sur la vie privée pour tout nouveau système d'information ou technologie de communication afin de donner un délai raisonnable pour un examen réalisé par le commissaire à l'information et à la protection de la vie privée, et afin que le dépositaire des renseignements médicaux dispose du temps nécessaire pour tenir compte des commentaires du commissaire lors des étapes de planification. Page 22*

Recommandation 8 : *Il faut remplir une évaluation des répercussions sur la vie privée chaque fois qu'une modification importante est apportée à une promulgation, un système, un projet, un programme ou un service qui demande de collecter, d'utiliser ou de communiquer des renseignements médicaux personnels. Je recommande également que l'Assemblée législative songe à modifier l'article 89 de la Loi sur l'information sur la santé afin d'exiger une utilisation des évaluations des répercussions sur la vie privée semblable à celle qui est rendue obligatoire au paragraphe 42.1 de la LAIPVP. Page 22*

Nous joindre



**Commissaire à l'information et à la protection de la vie privée
des Territoires du Nord-Ouest
C. P. 382
Yellowknife NT X1A 2N3**

Téléphone : 1-867-669-0976

Sans frais : 1-888-521-7088

Télec. : 1-867-920-2511

Courriel : admin@oipc-nt.ca

Site Web : www.oipc-nt.ca



**Le Commissariat se trouve au premier étage de l'immeuble Lang à Yellowknife.
L'immeuble se trouve au coin de l'avenue Franklin et de la 49^e rue, et l'entrée est sur Franklin.**