

Annual Report

2022 – 2023



Northwest Territories



OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER

NORTHWEST TERRITORIES



July 1, 2023

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, 2022, to March 31, 2023.

Your truly,

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

/af

Mailing Address: PO Box 382 Yellowknife NT X1A 2N3
Phone: (867) 669-0976 Toll-Free: (888) 521-7088 Email: admin@oipc-nt.ca

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>Incidence of 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 23
<u>Contact Us</u>	Page 24

Commissioner's Message



The past year has been busy and challenging. The number of new files decreased from the previous year, but many of last years' files remain open as they go through the review process. New privacy breaches filed under the *Health Information Act* decreased significantly. This may, at least in part, be due to better privacy protection measures being in place within health information custodians and public bodies. It may also be due in part to the dissolution of the COVID-19 Coordinating Secretariat, which reported a significant number of privacy breaches over its short existence. Inasmuch as most of the recommendations in review reports issued under the *Health Information Act* in the last few years have been accepted, it is reasonable to expect some reduction in the incidence of privacy breaches. It is perhaps a bit early to draw any firm conclusions, but there is room for optimism.

The number of files proceeding under the *Access to Information and Protection of Privacy Act* has also decreased. The number of complaints about delay has started to increase while the number of applications by public bodies for extensions of time have been decreasing. The Access and Privacy Office (APO) has been the designated Coordinator to receive and process access to information requests for all government departments and the NWT Housing Corporation since March 2021.¹ In July 2022, I learned that, in approximately half of all requests, the public bodies do not respond within the statutory time periods. As I discuss further below, the number of trained personnel in the APO is insufficient. This situation requires rectification.

The difficulty in providing timely, accurate responses to access to information requests is not unique to the Northwest Territories.² In my view, the public bodies need to allocate more resources for access to information activities: action is required, not complacency. Public

¹ So designated per section 68.1 of the Act.

² See news reporting at <https://www.theglobeandmail.com/canada/article-secret-canada-investigation-backstory/>

bodies undoubtedly have other policy priorities competing for resources, but complying with the *Access to Information and Protection of Privacy Act* is not a policy option: it is a legal obligation.

When complaints reach our office, we first determine whether some informal resolution is possible.³ Not infrequently, a concern regarding the contents of a response to an access to information request, or to a possible breach of privacy, can be resolved through discussion and without the need for a formal review. Sometimes, individuals who are unfamiliar with the legislation simply need assistance to understand the legislation or how best to achieve their objectives. Wherever possible, and where appropriate, we attempt to facilitate early resolution.

On an operational note, our office is undergoing some changes in office space and in personnel. To accommodate staffing increases and the commensurate need for more appropriate office space, the Legislative Assembly recently agreed that a change in venue would be appropriate. The process for finding new space has begun and we expect to complete the move in the 2023-24 fiscal year and with minimal interruption in client service. In January of 2022 our new Investigator position was staffed; in late fall last year our Assistant Commissioner, Dylan Gray, announced he would be retiring early in the new year. Dylan's detailed, extensive knowledge of the *Health Information Act* and strong passion for protecting privacy made him a tremendous asset to the office. We wish Dylan all the best and thank him for his hard work and service.



³ This is specifically contemplated in section 144 of the *Health Information Act*.

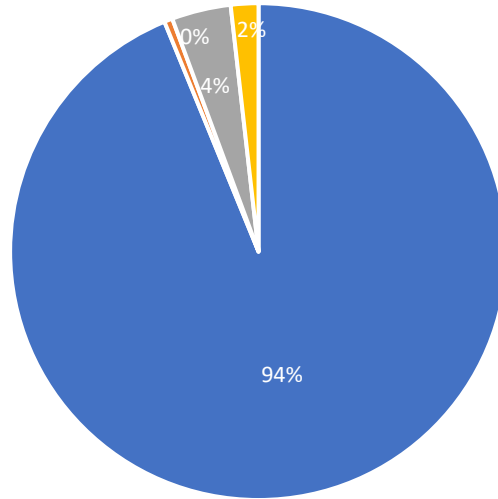
Financial Report

The total amount spent to operate the Office of the Information and Privacy Commissioner (OIPC) of the Northwest Territories for the fiscal year 2022/2023 was \$ 736,202.84. A detailed breakdown is outlined in the charts on the next page.

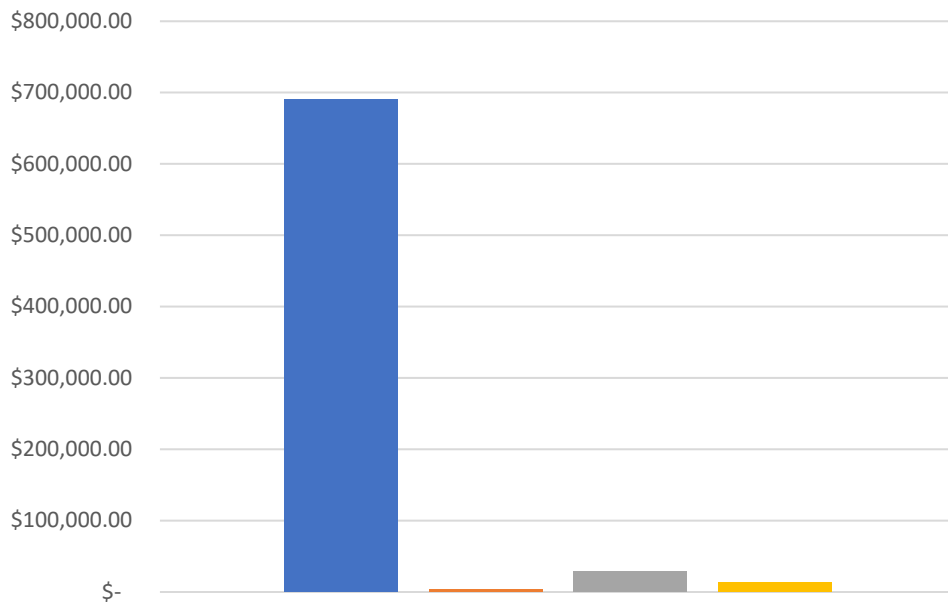
The administration of the OIPC budget was again uneventful. This years total operating budget was \$ 822,000.00 and we returned \$ 85,797.16 to the Legislative Assembly. There were a few circumstances affecting variances between actual and budgeted amounts, and a few other notable circumstances affecting finances:

1. Funds returned to the GNWT were mostly from unused money budgeted for Travel to conferences and related expenses for hotels, transportation and per diems. As professional conferences have largely resumed as in-person events, we expect this budget line to be more fully utilized going forward.
2. Professional development and training for staff is a continuing expense. Our Investigator and Assistant Commissioner were both enrolled in on-line courses through the University of Alberta.
3. Our office continues to use the services of a consultant to assist with reviewing Privacy Impact Assessments. The number of new assessments submitted for review decreased this year and therefore we did not use all the allotted funds. This is a fluctuating source of work-demand, but with the new requirement for privacy impact assessments under the *Access to Information and Protection of Privacy Act*, we expect this to be a significant resource draw. We will be monitoring this activity closely.
4. All workstations received an upgrade to the office computer set up which has improved workflow and efficiency.
5. New office space is being arranged for this year, and we expect some additional expenses related to moving and fit-up requirements.
6. Our Assistant Commissioner/Investigator retired in 2023. We are engaged in the recruitment process to find a replacement for this position, and hope to have the position filled by the summer/fall of 2023.

**Office of the Information and Privacy
Commissioner of the Northwest Territories
2022 / 2023 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*⁴ (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*.⁵ With the amendments that came into force in 2021, municipalities may be designated as public bodies by regulation.⁶

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 specific, limited 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 a process for members of the public to obtain access to such records. Part 2 governs public bodies' collection, use, and disclosure of individuals' personal information. Amendments to the *Act* that came into force in 2021 provided additional privacy breach response requirements and introduced privacy impact assessment requirements.⁷

The Commissioner provides independent review of public bodies' decisions and actions under both Parts of the *Act*. After investigating the facts and receiving representations from the applicant or complainant, from the public body, and from any third parties, the Commissioner will issue a review report. A report may contain one or more orders or recommendations. A

⁴ SNWT 1994, c 20.

⁵ Subject to limitations and exceptions set under ATIPPA or other legislation.

⁶ No communities have yet been designated.

⁷ Substantial amendments were passed in SNWT 2019 c.8 and came into force on July 30, 2021.

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. 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. Protecting the public’s right of access to information and applying the relevant statutory exceptions can involve potentially complex decisions. Independent oversight helps to ensure public bodies apply the *Act* correctly, helping to assure applicants that their rights are being upheld.

The Health Information Act

The *Health Information Act*⁸ (*HIA*) governs the collection, use and disclosure of personal health information. It codifies the right of individuals to access their personal health information, the obligation of health information custodians to safeguard individual privacy and ensures that personal health information is available to support the provision of health care services. 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 Tłı̨chq̓ Community Services Agency, and private physicians and pharmacists operating in the Northwest Territories.

The *HIA* requires 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. Underlying 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 the health service provider “needs to know” to do their job.

The *HIA* also requires health information custodians to notify affected individuals⁹ 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.¹⁰ The Commissioner may initiate an investigation of a privacy breach upon the request of an individual who believes their personal health information was collected, used, or disclosed in contravention of the *Act*, or, in appropriate circumstances, the Commissioner may initiate a review independently. After conducting a review, the Commissioner will prepare a report and may make recommendations to the health information custodian. The health information custodian must notify the Commissioner of the health information custodian’s decision to follow [or not to follow] the recommendation(s)

⁸ SNWT 2014, c 2.

⁹ Section 87 of the *Health Information Act*.

¹⁰ Section 87 of the *Health Information Act* and Section 15(2) of the *Health Information Regulations*.

within 30 days of receiving a report. Further, the health information custodian must comply with a decision to follow the Commissioner's recommendation within 45 days of 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's powers, duties and functions set out under the *Access to Information and Protection of Privacy Act (ATIPPA)* and the *Health Information Act (HIA)* are carried out through the Office of the Information and Privacy Commissioner (OIPC). The Commissioner's primary functions involve receiving and reviewing complaints about breaches of privacy and about the adequacy of public bodies' responses to access to information requests.

The Commissioner will also review and comment on Privacy Impact Assessments (PIAs) that are submitted to the Office of the Information and Privacy Commissioner. 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 identify where policies or programs align with legislative requirements and identify gaps or weaknesses that may require resolution *before* implementation. PIAs have been required under the *HIA* since it came into force in 2015, since 2019 under the GNWT's Protection of Privacy Policy 82.10, and since 2021 under the ATIPPA.

In addition to PIA's, the Commissioner may also review and comment on proposed legislation regarding possible implications for privacy protection or access to government information.

The Year in Review

The Office of the Information and Privacy Commissioner opened a total of 177 files in the fiscal year 2022/2023. Of these, 57 were matters within the scope of the *Access to Information and Protection of Privacy Act* and 120 are governed by the *Health Information Act*.

Overview of the Numbers

Access to Information and Protection of Privacy Act (ATIPPA)

The OIPC opened 57 files under the *Access to Information and Protection of Privacy Act* between April 1, 2022, and March 31, 2023:

Request for Review – Challenging redactions made in access response	4
Request for Review – Fees, Delays, Extensions or Refused access	8
Request for Review – A 3 rd Party requests a review	1
Request for Review – Breach of Privacy complaint	7
Request for Review – Correction to records	1
Request for Time Extension for Public Body to respond to access request	19
Notification from Public Body - Breach of Privacy	12
Consultations/Comments – Acts, Legislations, Bills, PIA's	4
Miscellaneous and Administrative	1

Health Information Act (HIA)

The OIPC opened 120 files under the *Health Information Act* between April 1, 2022, and March 31, 2023:

Notifications from Public Body - Breach of Privacy	105
Request for Review – Privacy Issues and Complaints	2
Comments – Privacy Impact Assessment (PIA)	9
Comments – Health Policies, Acts, Processes	1
Miscellaneous and Administrative	1
Special Projects or OIPC initiated Reviews	2

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 were not followed. The following matters are relevant to these requirements, and I also include some separate recommendations for consideration by the Legislative Assembly.

Review Reports

Our office issued thirty-one review reports under the *Access to Information and Protection of Privacy Act (ATIPPA)* in 2022/2023. Twenty reports dealt with public bodies' applications for extensions of time to respond to access to information requests. Seven reports reviewed public bodies' responses to access to information requests. Four reports reviewed allegations that personal information had been collected, used, or disclosed without legal authorization.

Review reports are publicly available on-line at <https://www.canlii.org/en/nt/ntipc/>.¹¹

The Commissioner may issue orders at the conclusion of reviews. These orders are binding on public bodies. To monitor compliance, orders will direct the public body to report back to our office on its compliance activity. Thus far, we have not identified any compliance issues.

The Commissioner may still make formal recommendations for a public body's consideration when dealing with privacy breaches involving personal information.¹² If a privacy breach is "material"¹³ 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 decides whether to follow any recommendation and reports to the Commissioner regarding the implementation of any accepted recommendations. My office did not receive a notice or report regarding a personal data breach under Division E this past year.

Time Extension Requests

My office received twenty extension-of-time requests from public bodies and issued nineteen extension Review Reports between April 1, 2022, and March 31, 2023. This is a relatively 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," subject to review by my office upon request.

¹¹ Past years' decisions are also available on-line on this free public database.

¹² Division E of Part 2 of *ATIPPA*

¹³ The *Act* does not define this term but there are factors to consider set out in subsection 49.9(2).

Formal review reports for such situations were infrequent. 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 process for extending time periods has 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 first, the Act deems this a refusal to respond.¹⁴

Time extensions for third-party consultation

Fifteen Extension Review Reports addressed requests for time extensions to accommodate public bodies' consultation with third parties. Consultation is required where third-party personal information could be disclosed in a response to the access to information requests. Third-party consultation requires 55 business days to complete.¹⁵ In every case this will exceed the 20 business-day extension available under subparagraph 11(1)(c), and therefore requires an extension authorization by the Commissioner under section 11.1.

In the normal course, where the public body requires a 55 business-day extension to conduct third-party consultation, there is no basis for the IPC to deny an authorization and the authorization process is essentially a 'rubber stamp'. In my view, this process 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.*

Delay in responding to access to information requests

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 2021 amendment, a public body could rely on this provision to grant itself an extension of time of a "reasonable period" to respond to an access request, 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 Government of the Northwest Territories (GNWT) has created the Access and Privacy Office (APO) to provide support to all GNWT departments¹⁶ 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,

¹⁴ See section 8(2) of the *Access to Information and Protection of Privacy Act*

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

¹⁶ And the Northwest Territories Housing Corporation

helping to bring critical knowledge and experience and efficiency to the access to information process.

Over the year, I received two requests from public bodies for a 20 business-day extension of time and three other requests for longer extensions to deal with large volumes of records. During this period there has been an increase in the number of complaints to our office of delay from applicants awaiting responses to their access to information requests. The APO says that when it is unable to respond to an access request in the time allowed it will often not seek an extension of time to respond but rather apply its limited time resources to the task of preparing the response on behalf of the public body. This is, in a sense, a pragmatic approach to dealing with the problem of having insufficient resources to provide a response within the time periods set by the Act: the task of applying for a time extension will slow response time further by drawing away limited resources from the task of providing the actual response. However, this approach confuses the public's reasonable expectations about process and response times, and it ignores the requirements of the legislation.

In July 2022, I accompanied a representative of the APO to a meeting with senior GNWT officials. The APO representative advised the group that responses to access requests were being provided late slightly more than 50% of the time. I do not believe the APO is solely responsible for the delays; I am advised that delay is sometimes exacerbated by the public body taking too long to review and approve a response. In my view, the Access and Privacy Office is a good administrative mechanism for the GNWT to provide access to information to the public. Having dedicated resources and trained, experienced staff is better than having access to information dealt with from 'the corner of the desk' of public bodies' employees who are already in full-time positions. However, without sufficient resources, this mechanism will not function properly, and it is apparent that the APO is not staffed sufficiently to adequately assist public bodies discharge their legal obligations in a timely way.

Legally, delays are the responsibility of the public bodies. Among the 2021 amendments were provisions that shortened the timelines for responses and created new authorization requirements for time extensions. The APO confirmed recently that its staffing level has not changed since 2022 and, not surprisingly, response times have not improved. It appears that public bodies are relying on the APO's assistance without ensuring the APO is sufficiently resourced and despite knowing that responses are being provided late at least half of the time. In such circumstances, relying on the APO to discharge legal obligations is not reasonable. It also appears to be out of step with the direction provided by the legislature, which is to decrease the waiting time between the submission of an access to information request and the receipt of the response.

The government has previously 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.”¹⁷ This is a statement of intent; however, without sufficient resources, human and otherwise, the APO will not be able to adequately support the government departments to discharge their statutory obligations.

Recommendation 2: *The public bodies should review their legal obligations to respond to access to information requests and evaluate their capacity to provide responses within the legislated time periods. They should also ensure, either collectively or individually, that the APO is appropriately resourced so that it can reliably assist public bodies to respond to access to information requests within the legal time periods and to comply with the relevant procedural requirements.*

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 Department of Justice included this office in its public consultation process regarding proposed Missing Persons Legislation, and the Legislative Assembly provided the opportunity to comment on two other pieces of legislation. I trust that the comments were of some utility, and I look forward to reviewing future draft legislation.

Timelines in ATIPPA

Prior to the 2021 amendments to *ATIPPA* coming into force, the *Act* stated a review must be completed within 180 days of receipt of a request for review.¹⁸ This period is now 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 prior to 2021 was just over 12 months -- significantly more than 180 days. Our new Investigator came onboard in January 2022. That position was approved in 2020 based on increases to the file load that had already occurred. While OIPC staffing increased from three to four people (including the Commissioner), the number of files coming into the office 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. While it may be useful for the *Act* to set a ‘benchmark’ timeline for completing a review, it would help clarify expectations of the review process if the *Act* expressly stated that the Commissioner could extend the period for completion of a review.

¹⁷ 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

¹⁸ See section 31(3).

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 thirteen 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 on-line 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 were accepted by the health information custodians.

Alternative Resolutions

Privacy breaches may be addressed through a formal review when an individual requests a review or if the Commissioner determines this to be a useful approach.¹⁹ Another approach 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. Alternative approaches are generally well received by custodians, and informal resolutions have led custodians to develop measures to prevent privacy breaches and to respond better to breaches when they occur. Where appropriate, I will continue to employ such alternative approaches to resolving privacy breaches.

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

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.²² It would be helpful to have a required reporting process on the implementation of recommendations.

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.

²² 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.

Recommendation 4: *The Department of Health and Social Services 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.*

A Recommendation not accepted

The *Health Information Act* requires the annual report to identify any recommendations made in a review that are not accepted by a health information custodian. This year there was only one instance of this: in a review²³ dealing with a doctor taking the wrong prescription from a shared printer and giving it to the wrong patient, I recommended that NTHSSA install individual printers in examination rooms – the intent being to put the ‘prescription pad’ back into the privacy of the examination room. NTHSSA did not accept the recommendation, but indicated it was continuing “to explore technology and equipment improvements for its operations that balance privacy safeguards, infection prevention and control safeguards and operations.

In follow-up discussion with NTHSSA I learned that NTHSSA is pursuing the solution of individual printers in examination rooms. It agrees this is a good privacy safeguard and it is currently working on procuring the appropriate printers that meet regulations for health precautions. The decision to not accept the recommendation was based on the concern that putting a printer in all examination rooms is a significant practical obstacle in some existing health care facilities; however, I understand that examination rooms in new and planned facilities will be so equipped. The recommendation was not accepted in full, but neither was it rejected in full.

Incidence of Privacy Breaches

The number of new *Health Information Act* files decreased from 234 last year to 120 this year, and the number of privacy breach notifications from health information custodians decreased from 206 to 105. This is a significant improvement from the past year, though still approximately 30% higher than the year before that.

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)

COVID Secretariat

Last year there were over 55 privacy breach notifications received from the COVID Secretariat. The Secretariat ceased operations in April 2022, and we received only one new privacy breach notice this fiscal year. Addressing these privacy breaches has been challenging. Many of the final breach reports were provided months after our office was notified, often missing pertinent

²³ [Yellowknife Primary Care Centre \(Re\)](#), 2023 NTIPC 23 (CanLII)

information, and answers to follow-up questions have often been provided months later. A frequent problem our office has encountered is the absence of records for some aspects of the Secretariat's operations: despite being a unit within the Department of Health and Social Services there were few or no records kept of the privacy training for personnel, although such records are required under the Department's *Mandatory Training Policy*. This is difficult to understand as the Secretariat was created as a unit within the Department²⁴ and the Department had relevant policies already developed to support compliance with the *Health Information Act*. The *Mandatory Training Policy* and the *Privacy Breach Policy* were created pursuant to a 2017 Ministerial Directive, and they bind all of the Department's employees. For reasons that remain unarticulated, the Secretariat did not act pursuant to these policies, nor does it appear that the Secretariat felt bound by them.

The Department advises that the Secretariat was, somehow, separate from the Department and that the Secretariat had not yet developed its own policies to address issues such as privacy training and privacy breach response. Why the Department's existing policies did not apply to the Secretariat is a conundrum. No real clarification or explanation has been offered beyond a general contention that the Secretariat was 'separate' from the Department. In my view this is a specious proposition and one which may have led to some confusion about privacy training requirements and proper privacy breach response. The Department had legal obligations as a health information custodian under the *HIA* and the policies that were promulgated to support compliance with the *HIA* apply to all parts of the Department.

In the government's report "Learning from the Response to COVID-19"²⁵ there is no discussion of the privacy breaches that occurred within the Secretariat, nor is there any discussion of the decision to situate the Secretariat within an existing health information custodian. There is no mention of the *Health Information Act* and the importance of protecting personal health information from unauthorized collection, use, or disclosure. Mistakes such as privacy breaches are perhaps inevitable when responding in a crisis, and I acknowledge that the many people who worked at the Secretariat performed valuable service to the residents of the Northwest Territories. However, the government should not forgo the opportunity now to take note of the legal and policy framework governing personal health information and take steps to prevent similar privacy breaches from occurring in any future pandemic.

Recommendation 5: *The GNWT should review the need for privacy-protective policies and procedures to support a specialized emergency response such as the COVID-19 Coordinating Secretariat and ensure it is equipped to operate within the bounds of the Health Information Act.*

NTHSSA

Most of the 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. The number of breach notifications is approximately half the previous

²⁴ https://www.gov.nt.ca/sites/flagship/files/documents/backgrounder_-_covid-19_coordinating_secretariat_final.pdf

²⁵ <https://www.gov.nt.ca/en/newsroom/gnwt-releases-covid-19-lessons-learned-report>

year's number,²⁶ but it is a 50% increase from 2 years ago.²⁷ The longer term trend is still increasing rates of privacy breach reports. Privacy breaches have frequently occurred while sending personal health information via fax²⁸, when sending emails, printing documents, and using electronic health information systems. Breaches have also occurred when documents have been lost on a public walkway²⁹ or when records have been accessed by employees for unauthorized reasons.³⁰

NTHSSA has taken steps to improve awareness amongst staff about recognizing and responding to breaches, and its reporting process also seems to be improving. The number of privacy breach notices indicates there is more work to be done in applying the appropriate administrative, technical, and physical safeguards to protect personal health information. Despite the recurring nature of some types of privacy breaches, it does appear that the NTHSSA is striving to improve its ability to discharge its legal obligation to protect the confidentiality of the personal health information under its custody and control.

Recurring Issues in Privacy Breaches

Faxing

Though the circumstances may differ somewhat, the types of breaches reported are largely unchanged from previous years. Email continues to be an increasing source of privacy breaches, followed by misidentification of patients and their records and failure to apply reasonable security measures to paper records. Faxing remains a significant source of privacy breaches. There were 21 privacy breach notifications (20% of the breach notices) this fiscal year regarding faxing errors.

The incidence of unauthorized disclosure of personal health information when using fax machines has been addressed in past review reports and Annual Reports.³¹ Faxing has also been the subject of comment by the Standing Committee on Government Operations.³² The GNWT has previously advised it intends to reduce 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.”³³

²⁶ 206 Breach notifications

²⁷ 66 Breach Notifications

²⁸ Approximately 20% of the breach notifications were for faxing errors.

²⁹ Northwest Territories Health and Social Services Authority (Re), 2022 NTIPC 19 (CanLII), <https://canlii.ca/t/jtrzr>

³⁰ Northwest Territories Health and Social Services Authority (Re), 2022 NTIPC 13 (CanLII), <https://canlii.ca/t/jt9r9>

³¹ 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>

³² 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_commissionio.pdf

³³ 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

In 2022, the NTHSSA created a system-wide policy regarding faxing of patient information. This policy states “only information which is urgent for the continuity of patient care should be transmitted by fax.” This is a useful restriction on the use of facsimile transmission; however, the same restriction appears in the predecessor policy document from 2011.³⁴ There are some differences between the two policy documents, and many similarities. Whether a new policy will have a significant effect on the incidence of privacy breaches remains to be seen.

The OIPC will continue to monitor this issue.

Recommendation 6: *Health information custodians should continue to reduce or eliminate the use of fax machines to transmit personal health information.*

Vigilance required when using email

The incidence of privacy breaches involving improper use of email has been increasing. Unauthorized disclosure can easily occur if an employee sends personal health information in an email to the wrong email address or to the wrong email group, or if they attach the wrong documents to an email. Emails that should have been messages to individuals have been mistakenly sent to large numbers of persons due to using “cc” instead of the “bcc” function. Inattention to detail is often the mistake that leads to such 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. These security measures are already specified to some degree in the *Electronically Stored and Transferred Information Policy*. As mentioned previously, proper privacy training is essential to ensuring that employees are aware of the applicable privacy protective measures.

Recommendation 7: *Health information custodians should utilize secure electronic transmission measures when transmitting personal health information.*

Privacy Training

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. Training in privacy protective policies and procedures is essential to creating a privacy-protective workplace culture.

The Department of Health and Social Services (DHSS) created its *Mandatory 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 to respond appropriately in the event of a breach.

Employees acting in positions without appropriate privacy training, and management inadequately documenting training, continue to be issues. Custodians will often address training

³⁴ Stanton Territorial Health Authority’s Facsimile Transmission of Patient Information policy dated January 2011.

deficiencies as part of their response to breach events, but this should not be necessary if custodians comply with the *Mandatory Training Policy*. Adequate employee training requires the dedication of resources and requires on-going support from leadership and management.

Recommendation 8: *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.*

Privacy Impact Assessments

This year our office reviewed and commented on nine Privacy Impact Assessments (PIAs) submitted by the DHSS and by the NTHSSA. Several of the PIAs addressed health information management and communications systems intended to support the government's response to the COVID pandemic.

The *HIA* requires a PIA to identify potential privacy risks posed by new health care information and communication systems, or changes thereto.³⁵ The Act also allows the Commissioner to comment on a PIA,³⁶ presumably so the custodian can reflect on those comments when finalizing 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) may make it difficult to make changes to improve privacy-protective safeguards. A PIA review should be completed well before project implementation, and certainly before any personal health information is subjected to the system and used operationally.

These are documents that take significant time to prepare, and reviewing a PIA also requires time – it is not a 'check-box' activity. Some PIAs have arrived in our office only days before the proposed project or system was scheduled to be implemented. Such timing suggests that the review of a PIA by this office is 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.

PIAs are being submitted; however, more work needs to be done to utilize the PIA as part of project design. Unfortunately, the *HIA* does not address when a PIA is to be completed, or when it should be provided to the Commissioner, or even whether the Commissioner's comments need be considered. Practically speaking, however, a PIA should be completed and provided for review and comment at an early stage of project development so that any comments from the Commissioner can be considered and incorporated into project design where appropriate.³⁷ I note that amendments to the *ATIPPA* now expressly address these requirements for PIAs.³⁸

³⁵ Section 89

³⁶ Section 175

³⁷ 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

³⁸ See section 42.1 of *ATIPPA*

Recommendation 9: Privacy Impact Assessments addressing any new information system or communication technology that involves the collection, use or disclosure of personal health information should be completed and submitted so that there is a reasonable period for review by the Information and Privacy Commissioner and for any comments to be considered by the health information custodian in the planning stages before implementation.

Recommendation 10: The Legislative Assembly should consider amending section 89 of the Health Information Act to include similar provisions regarding privacy impact assessments as mandated in section 42.1 of the ATIPPA.



Interjurisdictional Activity

The Federal, Provincial, and Territorial (FPT) Information and Privacy Commissioners continue to meet regularly online to share information, hear presentations, and discuss policies, technology, legislative proposals, and various other topics and issues pertaining to access to information and privacy protection. These meetings are a valuable forum to stay informed of policy developments at the national and international level.

The annual Information and Privacy Commissioners' conference was held in person in St. John's, NL in September 2022. In addition to receiving jurisdictional reports and several presentations on emerging issues, the conference finalized a resolution regarding the securing of public trust in digital health care. The resolution can be found at: https://priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_220921/.

In November 2022, a second annual Investigators' Conference took place online. Both our office's Assistant Commissioner and Investigator participated in what was both a skill-based and knowledge-based learning event. By all accounts, it was a beneficial experience and our office will be attending again this year.

Final Thoughts

The right to privacy – the right to be let alone, to be free from intrusion or interference from others, including the state – is a fundamental right with a constitutional footing in section 8 of the *Canadian Charter of Rights and Freedoms*. The *Access to Information and Protection of Privacy Act* and the *Health Information Act* legislate specific privacy protections with respect to personal information held by our public government institutions.

When governments supply services to individuals, personal information is inevitably collected, used, and sometimes disclosed. As the digitalization of government services increases, electronic collection of personal information data – which is already significant – will continue to increase. Creating, using, and storing electronic data can create significant efficiency gains for governments in providing services to citizens. I am not alone in appreciating the convenience of renewing my driver's license and vehicle registration with the click of a few buttons rather than waiting in line at a registry office.

But, these gains are often accompanied by an increase in the risk of unauthorized use or disclosure. Personal information data sets can be the targets of bad actors engaged in ransomware or identity theft, and public governments are often the targets of such bad actors. Government must monitor the risk environment and protect those electronic systems containing personal information with reasonable security measures, i.e., privacy-protective system design, encryption, passwords, virtual private networks, secure file transfer protocols, user training, privacy-protective policies and procedures, regular auditing, and oversight, etc. Good privacy protection requires significant effort!

New threats are emerging. Many are raising concerns about 'Artificial Intelligence', both as a threat to privacy and as an existential threat. As the categories and sophistication of potential threats to privacy continue to grow, the effort and resources required to counter the threats must also grow. The government of the Northwest Territories has not suffered a major cyberattack, such as experienced by the government of Nunavut in 2019 or the government of Newfoundland's health care system in 2021, but the potential threat is clear and present. Every public body and health information custodian should be assessing its security measures and ensuring a strong defense to protect the personal information in their care and control.

It is fair to observe that extra layers of security can subtract from the potential efficiency gains. Sometimes, security measures such as passwords can be viewed as obstacles to efficiency; that is, until a privacy breach occurs. In a review completed this year,³⁹ I learned that a public body had stored a significant number of employee files in the digital integrated information management system (DIIMS) without password protection or other appropriate security controls. The files were exposed to unauthorized access by unauthorized employees, and this unfettered access had been going on for an extended period. The public body's response involved significant and costly efforts: several employees dedicated months of their time to dealing with the breach. This breach is an instructive example for public bodies to consider when deciding on

³⁹ *Applicant A (Re)*, 2022 NTIPC 20 (CanLII), <https://canlii.ca/t/jtpkw>

the resources to devote to privacy-protective security measures: the cost implications, in both financial and human resources, of a privacy breach event can be very significant!

Going forward, I highly recommend that public bodies attend closely to the need for reasonable, effective security measures to protect the personal information entrusted to their care and control. Constant vigilance is essential.

Lastly, it is with great sadness that we note the passing of Ms. Elaine Keenan Bengts on August 8, 2022. After a long legal career which included serving the Northwest Territories and Nunavut as the first Information and Privacy Commissioner from 1997 to 2020, Ms. Keenan Bengts' plans for a well-deserved retirement were cut short by illness. Ms. Keenan Bengts had an inspiring, tireless passion for the work of this office and contributed much to the people of the Northwest Territories. She will be missed.



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: *The public bodies should review their legal obligations to respond to access to information requests and evaluate their capacity to provide responses within the legislated time periods. They should also ensure, either collectively or individually, that the APO is appropriately resourced so that it can reliably assist public bodies to respond to access to information requests within the legal time periods and to comply with the relevant procedural requirements. (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 Department of Health and Social Services 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 15)*

Recommendation 5: *The GNWT should review the need for privacy-protective policies and procedures to support a specialized emergency response such as the COVID-19 Coordinating Secretariat and ensure it is equipped to operate within the bounds of the Health Information Act. (Page 16)*

Recommendation 6: *Health information custodians should continue to reduce or eliminate the use of fax machines to transmit personal health information. (Page 18)*

Recommendation 7: *Health information custodians should utilize secure electronic transmission measures when transmitting personal health information. (Page 18)*

Recommendation 8: *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 19)*

Recommendation 9: *Privacy Impact Assessments addressing any new information system or communication technology that involves the collection, use or disclosure of personal health information should be completed and submitted so that there is a reasonable period for review by the Information and Privacy Commissioner and for any comments to be considered by the health information custodian in the planning stages before implementation. (Page 20)*

Recommendation 10: *The Legislative Assembly should consider amending section 89 of the Health Information Act to include similar provisions regarding 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 2022 – 2023



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

TERRITOIRES DU NORD-OUEST

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'ijahch'uu zhit yinohtan ji', diits'at ginohkhii.

Gwich'in

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.

Inuvialuktun

Ĉ'bdġ ǱǱ^{sb}Δ^c ΛϚLJΔ^{rc} Δ^{sb}Ǳġ^c ^{sb}ʔLǱǱ^b, Ɓ^cǱ^a Ɓ^c Ɓ^{sb}c^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



COMMISSARIAT À
L'INFORMATION ET
À LA PROTECTION
DE LA VIE PRIVÉE
TERRITOIRES DU NORD-OUEST

Le 1^{er} juillet 2023

M. Frederick Blake
Président de l'Assemblée législative
C. P. 1320
Yellowknife NT 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 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^{er} avril 2022 au 31 mars 2023.

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
Loi sur l'accès à l'information et la protection de la vie privée	
Loi sur les renseignements sur la santé	
Commissaire à l'information et à la protection de la vie privée	
<u>Bilan de l'année</u>	Page 9
Aperçu des chiffres (LAIPVP et LRS)	
Loi sur l'accès à l'information et la protection de la vie privée	
<i><u>Rapports d'examen</u></i>	
<i><u>Demandes de prolongation des délais</u></i>	
<i><u>Examens de projets de loi</u></i>	
<i><u>Délais prévus par la LAIPVP</u></i>	
Loi sur les renseignements sur la santé	
<i><u>Rapports d'examen</u></i>	
<i><u>Nombre de cas d'atteinte 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 22
<u>Dernières réflexions</u>	Page 23
<u>Résumé des recommandations</u>	Page 25
<u>Nous joindre</u>	Page 27

Message du commissaire



L'année écoulée a été chargée et exigeante. Le nombre de nouveaux dossiers a diminué par rapport à l'année précédente, mais de nombreux dossiers de l'année dernière restent actifs pendant la procédure d'examen. Les nouvelles atteintes à la vie privée relevant de la *Loi sur les renseignements sur la santé* ont nettement diminué. Cette baisse peut découler, du moins en partie, des mesures améliorées de protection de la vie privée en place chez les dépositaires de renseignements médicaux et dans les organismes publics. Elle peut également s'expliquer en partie par la dissolution du Secrétariat de coordination pour la COVID-19, qui a signalé un nombre important d'atteintes à la vie privée au cours de sa brève existence. Dans la mesure où la plupart des recommandations formulées dans les rapports d'examen publiés en vertu de la *Loi sur les renseignements sur la santé* au cours des dernières années ont été acceptées, on peut raisonnablement s'attendre à une certaine réduction du nombre de cas d'atteintes à la vie privée. Il est peut-être un peu tôt pour tirer des conclusions définitives, mais nous pouvons être optimistes.

Le nombre de dossiers traités en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* a également diminué. Le nombre de plaintes au sujet des délais a commencé à augmenter alors que le nombre de demandes de prolongation par les organismes publics a diminué. Depuis mars 2021, le Bureau de l'accès à l'information et de la protection de la vie privée (BAIPVP) est le coordinateur désigné pour recevoir et traiter les demandes d'accès à l'information de tous les ministères et d'Habitation TNO¹. En juillet 2022, j'ai appris que les organismes publics ne respectaient pas les délais de réponse prévus par la Loi pour environ la moitié des demandes. Comme je l'explique plus loin, le nombre de personnes formées au sein du BAIPVP est insuffisant. Cette situation doit être corrigée.

¹ Tel que prévu par l'article 68.1 de la Loi.

La difficulté de fournir des réponses rapides et précises aux demandes d'accès à l'information n'est pas propre aux Territoires du Nord-Ouest². À mon avis, les organismes publics doivent allouer davantage de ressources dans la sphère d'accès à l'information : il faut des mesures, non de la complaisance. Les organismes publics ont sans aucun doute d'autres priorités stratégiques pour lesquelles ils se disputent les ressources, mais le respect de la *Loi sur l'accès à l'information et la protection de la vie privée* n'est pas une option stratégique : c'est une obligation légale.

Lorsque des plaintes parviennent à notre bureau, nous commençons par déterminer si une résolution informelle est possible³. Il n'est pas rare qu'une préoccupation concernant le contenu d'une réponse à une demande d'accès à l'information, ou à une possible violation de la vie privée, soit résolue par la discussion et sans qu'un examen officiel soit nécessaire. Parfois, les personnes qui ne connaissent pas la Loi ont simplement besoin d'aide pour la comprendre ou pour connaître la meilleure façon d'atteindre leurs objectifs. Dans la mesure du possible, et le cas échéant, nous nous efforçons de faciliter une résolution rapide.

Sur le plan opérationnel, quelques changements s'opèrent à notre bureau en ce qui concerne l'espace de travail et le personnel. Pour faire face à l'augmentation des effectifs et au besoin de locaux plus appropriés qui en découle, l'Assemblée législative a récemment convenu qu'un changement de lieu serait approprié. Le processus de recherche de nouveaux locaux a commencé, et nous comptons terminer le déménagement au cours de l'exercice 2023-2024 tout en réduisant au minimum les interruptions du service à la clientèle. En janvier 2022, le nouveau poste d'enquêteur a été pourvu; puis à la fin de l'automne dernier, notre commissaire adjoint, Dylan Gray, a annoncé qu'il prendrait sa retraite au début de la nouvelle année. Les connaissances détaillées et approfondies de M. Gray sur la *Loi sur les renseignements sur la santé* et son grand intérêt pour la protection de la vie privée ont fait de lui un atout incroyable pour le bureau. Nous lui souhaitons le meilleur et le remercions pour son service et son travail soutenu parmi nous.



² Voir l'article suivant : <https://www.theglobeandmail.com/canada/article-secret-canada-investigation-backstory/>.

³ L'article 144 de la *Loi sur les renseignements sur la santé* prévoit expressément cette possibilité.

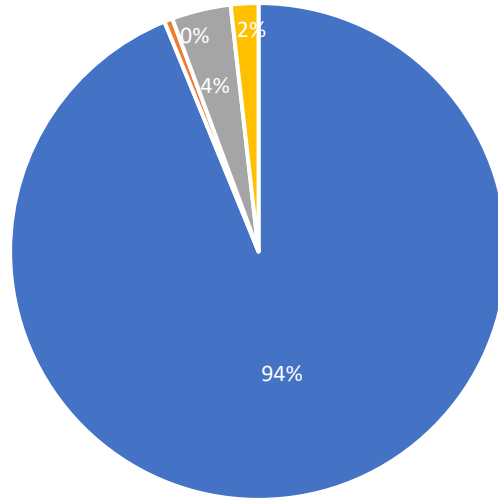
Rapport financier

Les dépenses d'exploitation du Commissariat à l'information et à la protection de la vie privée (CIPVP) des Territoires du Nord-Ouest (TNO) ont totalisé 736 202,84 \$ en 2022-2023. Vous pouvez trouver une ventilation détaillée de ces dépenses dans les tableaux de la page suivante.

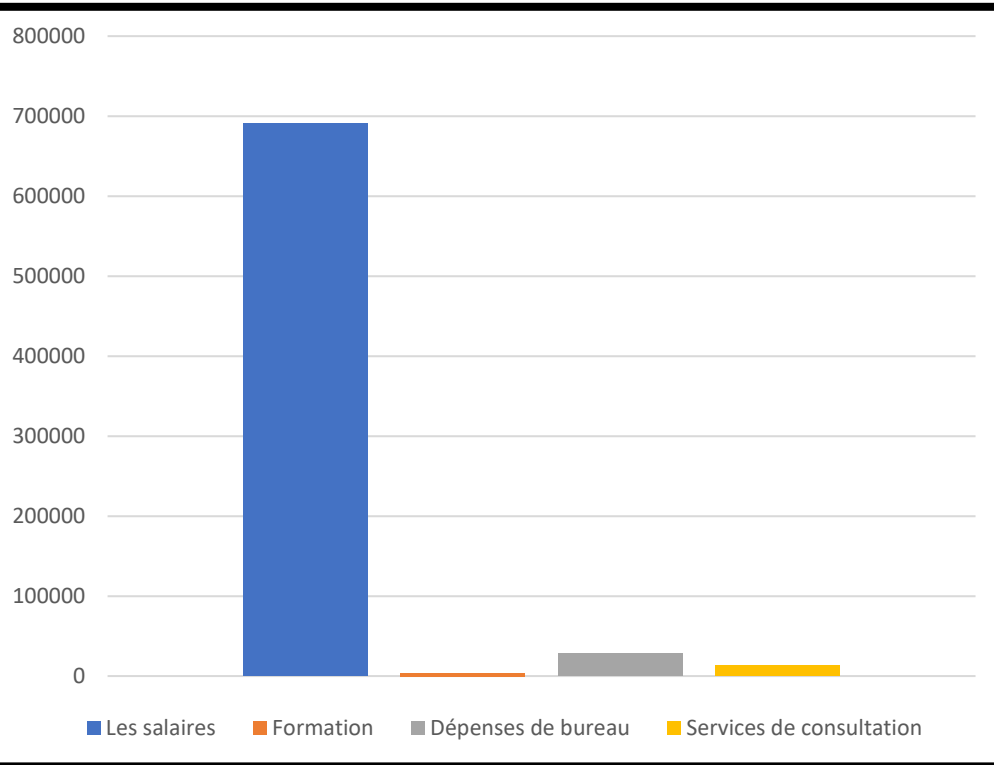
Encore une fois, la gestion du budget du CIPVP n'est associée à aucune difficulté. Cette année, le budget de fonctionnement total était de 822 000 \$ et nous avons remis 85 797,16 \$ à l'Assemblée législative. Quelques circonstances ont entraîné des écarts entre les montants réels et les montants prévus au budget, et d'autres circonstances notables ont touché les finances :

1. Les fonds reversés au gouvernement des Territoires du Nord-Ouest (GTNO) provenaient principalement de fonds non utilisés prévus au budget pour les déplacements vers des conférences et les dépenses connexes pour les hôtels, le transport et les indemnités journalières. Comme les conférences professionnelles ont largement repris sous la forme d'événements en personne, nous nous attendons à ce que cette ligne budgétaire soit davantage utilisée à l'avenir;
2. Nous poursuivons nos dépenses en formation et perfectionnement professionnel. Notre enquêteur et notre commissaire adjoint ont tous deux suivi des cours en ligne à l'Université de l'Alberta;
3. Notre bureau continue d'utiliser les services d'un consultant pour l'aider à examiner les évaluations des répercussions sur la vie privée. Le nombre de nouvelles évaluations soumises pour examen a diminué cette année, alors nous n'avons pas utilisé tous les fonds alloués. Ces évaluations sont une source fluctuante de demande de travail, mais en raison de la nouvelle exigence prévue par la *Loi sur l'accès à l'information et la protection de la vie privée*, nous nous attendons à ce qu'elles mobilisent beaucoup de ressources. Nous suivrons cette activité de près.
4. Tous les postes de travail au bureau ont bénéficié d'une mise à niveau de leur configuration informatique, ce qui a permis d'améliorer l'efficacité et la capacité de travail.
5. De nouveaux locaux sont en cours d'aménagement pour cette année, alors nous nous attendons à des dépenses supplémentaires liées au déménagement et à la configuration des lieux.
6. Notre commissaire adjoint/enquêteur a pris sa retraite en 2023. Nous sommes en cours de recrutement afin de trouver un remplaçant pour ce poste, et nous espérons qu'il sera pourvu d'ici l'été ou l'automne 2023.

Commissariat à l'information et à la protection de la vie privée des Territoires du Nord-Ouest
Dépenses 2022-2023



■ Salaires ■ Formation ■ Dépenses de bureau ■ Services de consultation



■ Les salaires ■ Formation ■ Dépenses de bureau ■ Services de consultation

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*⁴ (LAIPVP) s'applique aux ministères, aux directions et aux bureaux du gouvernement des Territoires du Nord-Ouest, ainsi qu'à 22 agences, conseils, commissions, sociétés et autres organismes publics désignés dans le règlement d'application de la Loi⁵. Compte tenu des modifications qui sont entrées en vigueur en 2021, les municipalités peuvent être vues comme des organismes publics aux termes de la réglementation⁶.

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 régit la collecte, l'utilisation et la divulgation par les organismes publics des renseignements personnels des individus. Les modifications apportées à la Loi qui sont entrées en vigueur en 2021 ont ajouté des exigences en matière de mesures

⁴L^{TN}-O 1994, ch. 20.

⁵Sous réserve des restrictions et exceptions figurant dans la LAIPVP ou une autre loi.

⁶À l'heure actuelle, aucune collectivité n'a encore été désignée ainsi.

d'intervention en cas d'atteinte à la vie privée et ont introduit des exigences en matière d'évaluation des répercussions sur la vie privée⁷.

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, il doit produire un rapport d'examen. Ce rapport peut contenir un ou plusieurs arrêtés ou recommandations. 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. 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. La protection du droit d'accès du public à l'information et l'application des exceptions statutaires pertinentes peuvent impliquer des décisions potentiellement complexes. Une supervision indépendante aide à s'assurer que les organismes publics appliquent la LAIPVP comme il se doit, et peut contribuer à garantir aux demandeurs que leurs droits sont respectés.

Loi sur les renseignements sur la santé

Loi sur les renseignements sur la santé⁸ (*LRS*) régit la collecte, l'utilisation et la communication de renseignements médicaux personnels. Elle codifie le droit des personnes d'accéder à leurs renseignements personnels sur la santé et l'obligation des dépositaires de renseignements médicaux de protéger la vie privée des personnes, et garantit que les renseignements personnels sur la santé sont disponibles pour appuyer la prestation de services de soins de santé. 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 t̄l̄j̄ch̄q̄ ainsi que les médecins et pharmaciens des TNO qui travaillent dans le privé.

La LRS exige des dépositaires de renseignements médicaux qu'ils prennent des mesures raisonnables pour protéger la confidentialité et la sécurité des renseignements personnels médicaux des personnes. 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

⁷D'importantes modifications ont été adoptées dans la LTN-O 2019, ch. 8 et sont entrées en vigueur le 30 juillet 2021. Bien que les lois des TNO accordent un droit d'accès aux documents du gouvernement, ce droit n'est pas inconditionnel.

⁸LTN-O 2014, ch. 2.

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 médicaux qu'ils avisent les personnes concernées⁹ 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 préjudice¹⁰. Le commissaire peut lancer une enquête sur une atteinte à la vie privée à la demande d'un particulier qui croit que ses renseignements médicaux ont été collectés, utilisés ou divulgués de manière à enfreindre la Loi ou, dans des circonstances appropriées, le commissaire peut ouvrir une enquête de sa propre initiative. 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 de renseignements médicaux doit communiquer au commissaire sa décision d'appliquer ou non les recommandations dans les 30 jours suivant la réception d'un rapport. De plus, le dépositaire 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.



⁹Article 87 de la *Loi sur les renseignements sur la santé*

¹⁰ Article 87 de la *Loi sur les renseignements sur la santé* et paragraphe 15(2) du *Règlement sur les renseignements sur la santé*.

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 conformément à la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et à la *Loi sur les renseignements sur la santé* (LRS) sont mis en application par le Commissariat à l'information et à la protection de la vie privée (CIPVP). Les principales fonctions du commissaire consistent à recevoir et à examiner les plaintes relatives aux atteintes à la vie privée et à l'adéquation des réponses des organismes publics aux demandes d'accès à l'information.

Le commissaire doit également examiner et commenter les évaluations des répercussions sur la vie privée (ÉRVP) soumises au CIPVP. Les ÉRVP 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. Ces évaluations permettent de déterminer dans quelle mesure les politiques ou les programmes sont conformes aux exigences législatives et de cerner les lacunes ou les faiblesses qui pourraient devoir être résolues *avant* la mise en œuvre. Les ÉRVP sont exigées en vertu de la LRS depuis son entrée en vigueur en 2015, depuis 2019 en vertu de la Politique de protection de la vie privée 82.10 du GTNO et depuis 2021 en vertu de la LAIPVP.

En plus des ÉRVP, le commissaire peut également examiner et commenter les projets de loi en ce qui concerne les 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 177 dossiers en au cours de l'exercice 2022-2023. Parmi ceux-ci, 57 étaient couverts par la *Loi sur l'accès à l'information et la protection de la vie privée* et 120 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^{er} avril 2022 et le 31 mars 2023, le CIPVP a ouvert 57 dossiers en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*.

Demande d'examen – Contestation des caviardages effectués dans la réponse à l'accès à l'information	4
Demande d'examen – Frais, retards, prolongations de délais ou accès refusés	8
Demande d'examen – Demandes de tierces parties	1
Demande d'examen – Plainte pour atteinte à la vie privée	7
Demande d'examen – Correction aux dossiers	1
Demande de prolongation du délai accordé à l'organisme public pour répondre à une demande d'accès	19
Avis d'un organisme public – Atteinte à la vie privée	12
Consultations et observations – Lois, règlements, projets de loi, ÉRVP	4
Questions diverses et administratives	1

Loi sur les renseignements sur la santé

Entre le 1^{er} avril 2022 et le 31 mars 2023, le CIPVP a ouvert 120 dossiers en vertu de la *Loi sur les renseignements sur la santé*.

Avis d'un organisme public – Atteinte à la vie privée	105
Demande d'examen – Questions et plaintes liées à la protection des renseignements personnels	2
Observations – Évaluation des répercussions sur la vie privée (ÉRVP)	9
Observations – Politiques, lois et processus en matière de santé	1
Questions diverses et administratives	1
Projets spéciaux ou examens initiés par le CIPVP	2

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

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 ses recommandations n'ont pas été appliquées. Les questions suivantes touchent ces exigences, et j'ai également fait quelques recommandations distinctes aux fins d'examen par l'Assemblée législative.

Rapports d'examen

Le Commissariat a produit 31 rapports d'examen en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) en 2022-2023. Vingt d'entre eux portaient sur des demandes d'organismes publics désirant une prolongation du délai accordé avant de devoir répondre à une demande d'accès à l'information. Sept rapports portaient sur un examen des mesures prises par les organismes publics en réaction à des demandes d'accès à l'information. Quatre rapports portaient sur un examen d'allégations selon lesquelles des renseignements personnels avaient été collectés, utilisés ou divulgués sans autorisation légale.

Les rapports d'examen sont accessibles au public en ligne au <https://www.canlii.org/fr/nt/ntipc/>¹¹.

Le commissaire peut produire des ordonnances à la conclusion des examens. Les organismes publics doivent appliquer ces ordonnances. Pour surveiller leur respect, des arrêtés exigeront aux organismes publics de rendre compte au Commissariat des mesures prises pour se plier aux 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 lorsqu'il traite des atteintes à la vie privée concernant des renseignements personnels¹². Si une atteinte à la vie privée est « importante »¹³, le dirigeant 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. Le dirigeant ou la dirigeante de l'organisme public doit décider s'il applique ou non les recommandations, puis faire état au commissaire des recommandations acceptées et mises en œuvre. Au cours de l'année écoulée, le Commissariat n'a reçu aucun avis ou rapport lié à une atteinte à la vie privée en vertu de la section E.

¹¹Les décisions de l'exercice précédent sont aussi disponibles en ligne sur la base de données publique gratuite.

¹² Section E de la partie 2 de la LAIPVP.

¹³ The Act does not define this term but there are factors to consider set out in subsection 49.9(2).

Demandes de prolongation des délais

Le Commissariat a reçu 20 demandes de prolongation des délais de la part d'organismes publics et a produit 19 rapports d'examen pour prolongation entre le 1^{er} avril 2022 et le 31 mars 2023. Il s'agit d'une catégorie relativement nouvelle de rapport d'examen. Avant le 30 juillet 2021, les organismes publics pouvaient prolonger durant une « période raisonnable » le délai dont ils jouissaient pour répondre à une demande d'accès à l'information, examiné sur demande par le Commissariat. Il était peu fréquent que de telles situations mènent à la production de rapports d'examen. 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, le processus a 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 délai doit être soumise avant l'échéance du délai en vigueur. Si le délai arrive à échéance en premier, il s'agit selon la Loi d'un refus de répondre¹⁴.

Prolongation du délai en vue de consulter une tierce partie

Quinze rapports d'examen pour prolongation ont été produits pour traiter des demandes de prolongation de délai pour permettre aux organismes publics de consulter une tierce partie. Une consultation est nécessaire lorsque des renseignements personnels concernant une tierce partie pourraient être divulgués en réponse aux demandes d'accès à l'information. La consultation d'une tierce partie prévoit une période de 55 jours ouvrables¹⁵. Cette période est dans tous les 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 de l'article 11.1.

En temps normal, si l'organisme public nécessite une prolongation de 55 jours pour consulter une tierce partie, le CIPVP n'a aucune raison de refuser une autorisation et le processus est en quelque sorte une « formalité administrative ». À mon avis, il faudra réfléchir à ce processus.

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.*

Retard de réponse aux demandes d'accès à l'information

L'alinéa 11(1)b) autorise une prolongation 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 en

¹⁴Voir le paragraphe 8(2) de la *Loi sur l'accès à l'information et la protection de la vie privée*.

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

2021, un organisme public pouvait faire appel à cette disposition afin d'obtenir une prolongation d'une « période raisonnable » pour répondre à une demande d'accès, 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.

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) afin d'aider tous les organismes et ministères du GTNO¹⁶ 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.

Au cours de l'année, j'ai reçu deux demandes de prolongation de 20 jours ouvrables de la part d'organismes publics et trois autres demandes de prolongation plus longue pour traiter un grand volume de dossiers. Pendant cette période, nous avons reçu plus de plaintes concernant des retards par des demandeurs en attente de réponse à leur demande d'accès à l'information. Le BAIPVP indique que lorsqu'il n'est pas en mesure de répondre à une demande d'accès dans le délai imparti, il ne demandera souvent pas de prolongation du délai de réponse, mais utilisera plutôt ses ressources de temps limitées pour préparer la réponse au nom de l'organisme public. D'une certaine manière, il s'agit d'une approche pragmatique pour résoudre le problème du manque de ressources pour fournir une réponse dans les délais établis par la Loi : le fait de demander une prolongation du délai ralentira encore plus le temps de réponse puisque des ressources limitées seront détournées de la tâche consistant à fournir la réponse elle-même. Toutefois, cette approche ne tient pas compte des attentes raisonnables du public en ce qui concerne le processus et les délais de réponse, et ignore les exigences légales.

En juillet 2022, j'ai accompagné un représentant du BAIPVP à une réunion avec des hauts fonctionnaires du GTNO. Le représentant a informé le groupe qu'un peu plus de 50 % des réponses aux demandes d'accès étaient fournies en retard. Je ne pense pas que le BAIPVP soit le seul responsable des retards; on m'a informé que ces retards sont parfois exacerbés par le fait que l'organisme public prend trop de temps pour examiner et approuver une réponse. À mon avis, le Bureau est un bon mécanisme administratif qui permet au GTNO d'assurer l'accès du public à l'information. Il est préférable de disposer de ressources dédiées et d'un personnel formé et expérimenté que d'avoir accès à des informations traitées sur un « coin de table » par des employés d'organismes publics qui occupent déjà des postes à temps plein. Cependant, sans ressources suffisantes, ce mécanisme ne fonctionnera pas correctement, et il est évident que le BAIPVP n'a pas assez de personnel pour aider les organismes publics à respecter leurs obligations légales dans les délais impartis.

Selon la Loi, les retards sont de la responsabilité des organismes publics. Parmi les modifications de 2021, on trouve des dispositions qui raccourcissent les délais de réponse et créent de nouvelles exigences d'approbations pour les prolongations de délai. Récemment, le BAIPVP a confirmé que ses effectifs n'avaient pas changé depuis 2022 et, comme on pouvait s'y attendre,

¹⁶Et la Société d'habitation des Territoires du Nord-Ouest.

les délais de réponse ne se sont pas améliorés. Il semble que les organismes publics comptent sur l'assistance du BAIPVP sans s'assurer que celui-ci dispose de ressources suffisantes et tout en sachant que les réponses sont fournies en retard au moins la moitié du temps. Dans de telles circonstances, il n'est pas raisonnable de s'appuyer sur le BAIPVP pour s'acquitter d'obligations légales. Ce mécanisme semble également contradictoire avec l'orientation donnée par l'Assemblée législative, qui est de réduire le temps d'attente entre la présentation d'une demande d'accès à l'information et la réception de la réponse.

Le gouvernement a déjà 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 ¹⁷ ». Il s'agit là d'une déclaration d'intérêt, mais s'il n'y a 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 de leurs obligations légales.

Recommandation 2 : *Les organismes publics devraient revoir leurs obligations légales de répondre aux demandes d'accès à l'information et évaluer leur capacité à fournir des réponses dans les délais impartis par la loi. Ils doivent également veiller, collectivement ou individuellement, à ce que le BAIPVP dispose de ressources suffisantes pour fournir une assistance fiable aux organismes publics afin qu'ils répondent aux demandes d'accès à l'information dans les délais légaux et se conforment aux exigences procédurales appropriées.*

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 ministère de la Justice a inclus le Commissariat dans son processus de consultation publique concernant la loi sur les personnes disparues, et l'Assemblée législative lui a donné la possibilité de formuler des commentaires sur deux autres textes législatifs. J'espère que ces commentaires ont été utiles et je serai heureux d'examiner de futurs projets de loi.

Délais prévus par la LAIPVP

Avant l'entrée en vigueur des modifications à la LAIPVP en 2021, la Loi prévoyait qu'un examen devait être réalisé dans les 180 jours suivant la réception d'une demande d'examen¹⁸. Cette période est maintenant de 90 jours ouvrables.

¹⁷ Tiré 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 2). Situé ici : https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf.

¹⁸Voir le paragraphe 31(3).

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 avant 2021 était légèrement supérieure à 12 mois, ce qui va bien au-delà des 180 jours. Nous avons accueilli notre nouvel enquêteur en janvier 2022. Ce poste a été approuvé en 2020 sur la base de l'augmentation de la charge de travail qui s'était déjà produite. Bien que le personnel du CIPVP soit passé de trois à quatre membres (en comptant 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. Même s'il peut 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 sur la santé

Rapports d'examen

Cette année, le Commissariat a publié 13 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 ont été acceptées par les dépositaires de renseignements médicaux.

Autres formes de règlement

Les atteintes à la vie privée peuvent faire l'objet d'un examen formel lorsqu'une personne en fait la demande ou si le commissaire estime qu'il s'agit d'une approche utile¹⁹. Une autre approche consiste à collaborer avec le dépositaire de renseignements médicaux en traitant une question au moyen d'un mode alternatif de règlement des différends²⁰ ou, de manière encore moins officielle, en formulant des commentaires et des orientations et en proposant des ressources pertinentes à prendre en compte. Ces autres approches suscitent généralement de bonnes réactions chez les dépositaires, et les formes de règlement informelles ont poussé ces derniers à élaborer des mesures pour prévenir les atteintes à la vie privée et pour mieux y répondre lorsqu'elles se produisent. Lorsqu'il est pertinent de le faire, je continuerai à utiliser cette approche pour résoudre les problèmes d'atteinte à la vie privée.

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 décision²¹. Selon la Loi, le défaut d'aviser le commissaire de sa décision dans les 30 jours sera interprété comme une décision de ne pas suivre les recommandations du commissaire.

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

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

²⁰Article 138.

²¹Article 156.

acceptées. Par comparaison, le paragraphe 49.14 de la nouvelle version de la LAIPVP crée une telle obligation²². Il serait utile d’avoir un processus obligatoire de communication d’information relative à la mise en œuvre des recommandations.

Recommandation 4 : *Le ministère de la Santé et des Services sociaux 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 qu’ils informent le commissaire de la mise en œuvre des recommandations acceptées.*

Recommandation non acceptée

La *Loi sur les renseignements sur la santé* exige que le rapport annuel fasse état des recommandations formulées lors des examens qui n’ont pas été acceptées par les dépositaires de renseignements médicaux. Cette année, une seule recommandation n’a pas été acceptée. Dans le cadre d’un examen²³ portant sur un médecin qui a pris la mauvaise ordonnance dans une imprimante commune et l’a remise au mauvais patient, j’ai recommandé à l’ASTNO d’installer des imprimantes individuelles dans les salles d’examen, l’objectif étant de ramener le « bloc d’ordonnances » dans l’intimité de la salle d’examen. L’ASTNO n’a pas accepté la recommandation, mais a indiqué qu’elle continuait à « étudier les possibilités d’amélioration de la technologie et de l’équipement pour ses activités qui permettent de maintenir un équilibre entre les mesures de protection de la vie privée, les mesures de prévention et de contrôle des infections et les activités ».

Lors d’une discussion subséquente avec l’ASTNO, j’ai appris que cette dernière travaillait à mettre en place la solution d’imprimantes individuelles dans les salles d’examen. Elle convient qu’il s’agit d’une bonne mesure de protection de la vie privée et se procure actuellement les imprimantes adéquates répondant aux réglementations en matière de précautions liées à la santé. La recommandation avait été rejetée en raison d’une préoccupation selon laquelle l’installation d’une imprimante dans toutes les salles d’examen constituerait un obstacle pratique important dans certains établissements de soins de santé existants. Toutefois, je comprends que les salles d’examen des nouveaux et futurs établissements seront équipées de la sorte. La recommandation n’a pas été acceptée dans son intégralité, mais elle n’a pas non plus été rejetée entièrement.

Nombre de cas d’atteinte à la vie privée

Le nombre de nouveaux dossiers relatifs à la *Loi sur les renseignements sur la santé* a diminué, passant de 234 l’année dernière à 120 cette année, et le nombre d’avis d’atteinte à la vie privée transmis par des dépositaires de renseignements médicaux a également diminué, passant de 206

²²49.14. 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.

²³ Voir le document (en anglais seulement) intitulé [Yellowknife Primary Care Centre \(Re\)](#), 2023 NTIPC 23 (CanLII).

à 105. Il s'agit d'une nette amélioration par rapport à l'année dernière, bien que ces nombres restent environ 30 % plus élevés que ceux d'il y a deux ans.

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 tļchq
- Administration des services de santé et des services sociaux des Territoires du Nord-Ouest (ASTNO)

Secrétariat pour la COVID-19

L'année dernière, le Secrétariat pour la COVID-19 a envoyé plus de 55 avis d'atteinte à la vie privée. Le Secrétariat a cessé ses activités en avril 2022, et nous n'avons reçu qu'un seul nouvel avis d'atteinte à la vie privée au cours du présent exercice. Il a été difficile de remédier à ces cas d'atteinte à la vie privée. Nous avons reçu beaucoup de rapports finaux sur les atteintes plusieurs mois après que le Commissariat en avait été informé, il manquait fréquemment des renseignements pertinents, et les réponses aux questions de suivi ont souvent été fournies des mois plus tard. Un problème que notre bureau a régulièrement rencontré est l'absence de dossiers pour certains aspects des activités du Secrétariat. Bien que ce dernier ait fait partie du ministère de la Santé et des Services sociaux, il n'y avait que peu ou pas de dossiers concernant la formation du personnel en matière de protection de la vie privée, alors que ces dossiers sont requis en vertu de la Politique sur la formation obligatoire du ministère. Cette situation est difficile à comprendre, puisque le Secrétariat a été créé en tant qu'unité au sein du ministère²⁴, qui avait déjà élaboré des politiques pertinentes pour assurer le respect de la *Loi sur les renseignements sur la santé*. La Politique sur la formation obligatoire et la Politique sur les atteintes à la vie privée ont été créées conformément à une directive ministérielle de 2017 et s'appliquent à tous les employés du ministère. Pour des raisons qui demeurent inexplicables, le Secrétariat n'a pas agi conformément à ces politiques et ne semble pas s'être senti concerné par celles-ci.

Le ministère indique que le Secrétariat était, d'une certaine façon, indépendant de lui et qu'il n'avait pas encore élaboré ses propres politiques pour répondre aux questions telles que la formation sur la protection de la vie privée et la réponse aux atteintes à la vie privée. La raison pour laquelle les politiques existantes du ministère ne s'appliquaient pas au Secrétariat est inexplicable. Aucune véritable clarification ou explication n'a été fournie autre que l'affirmation générale selon laquelle le Secrétariat était « indépendant » du ministère. À mon avis, il s'agit d'une proposition captieuse qui a pu entraîner une certaine confusion concernant les exigences en matière de formation sur la protection de la vie privée et la réponse adéquate aux atteintes à la vie privée. Le ministère avait des obligations légales en tant que dépositaire de renseignements médicaux en vertu de la *Loi sur les renseignements sur la santé*, et les politiques promulguées pour assurer le respect de la Loi s'appliquent à toutes les parties du ministère.

²⁴ https://www.gov.nt.ca/sites/flagship/files/documents/backgrounder_-_covid-19_coordinating_secretariat_final_fr.pdf.

Dans le rapport du gouvernement « Leçons apprises de la réponse à la pandémie de COVID-19 »²⁵, il n'est pas question des atteintes à la vie privée qui se sont produites au sein du Secrétariat ni de la décision de placer le Secrétariat au sein d'un dépositaire de renseignements médicaux existant. Il n'est pas fait mention de la *Loi sur les renseignements sur la santé* et de l'importance de protéger les renseignements personnels sur la santé contre la collecte, l'utilisation et la divulgation non autorisées. Les erreurs telles que les atteintes à la vie privée sont peut-être inévitables en cas de crise, et je reconnais que les nombreuses personnes qui ont travaillé au Secrétariat ont rendu de précieux services aux Ténos. Toutefois, le gouvernement ne doit pas laisser passer l'occasion actuelle de prendre note du cadre juridique et politique régissant les renseignements personnels sur la santé et de prendre des mesures pour éviter que de telles atteintes à la vie privée ne se produisent lors d'une autre pandémie éventuelle.

Recommandation 5 : *Le GTNO devrait examiner la nécessité d'adopter des politiques et des procédures de protection de la vie privée pour soutenir un groupe d'intervention spécialisée en cas d'urgence, comme le Secrétariat de coordination pour la COVID-19, et s'assurer qu'il est équipé pour mener ses activités dans les limites de la Loi sur les renseignements sur la santé.*

ASTNO

La plupart des avis d'atteinte à la vie privée 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. Le nombre d'avis est environ deux fois moins élevé que celui de l'année précédente²⁶, mais il a augmenté de 50 % par rapport à il y a deux ans²⁷. La tendance à long terme est toujours à l'augmentation du nombre d'avis. Les atteintes à la vie privée ont souvent eu lieu alors qu'on transmettait des renseignements médicaux personnels par télécopieur²⁸ ou par courriel, qu'on imprimait des documents et qu'on utilisait les systèmes électroniques d'information sur la santé. Des atteintes ont également été causées par la perte de documents dans des endroits publics²⁹ et l'accès non autorisé à des dossiers par des employés³⁰.

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 semble également s'améliorer. Le nombre d'avis reçus indique qu'il y a plus de travail à faire du côté de l'application de mesures de prévention appropriées sur les plans administratif, technique et physique afin de protéger les renseignements médicaux personnels. Malgré la récurrence de certains types d'atteintes à la vie privée, il semble que l'ASTNO s'efforce d'améliorer sa capacité

²⁵ <https://www.gov.nt.ca/fr/newsroom/le-gtno-publie-son-rapport-sur-les-lecons-apprises-de-la-pandemie-de-covid-19>.

²⁶ 206 avis d'atteinte à la vie privée.

²⁷ 66 avis d'atteinte à la vie privée.

²⁸ Environ 20 % des avis d'atteinte à la vie privée concernent des erreurs survenues lors d'envois par télécopieur.

²⁹ Tiré du document suivant (en anglais) : *Northwest Territories Health and Social Services Authority (Re)*, 2022 NTIPC 19 (CanLII), <https://canlii.ca/t/jtrzr>

³⁰ Tiré du document suivant (en anglais) : *Northwest Territories Health and Social Services Authority (Re)*, 2022 NTIPC 13 (CanLII), <https://canlii.ca/t/jt9r9>

à s'acquitter de son obligation légale de protéger la confidentialité des renseignements personnels sur la santé dont elle a la garde et le contrôle.

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. Le courriel demeure une source croissante 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 papier. La télécopie reste une source importante d'atteintes à la vie privée. Au cours du présent exercice, il y a eu 21 avis (20 % des avis d'atteinte à la vie privée) concernant des erreurs survenues lors d'envois par télécopieur.

Le nombre de cas de divulgation non autorisée de renseignements médicaux personnels à l'aide de télécopieurs a été traité dans des rapports d'examen et des rapports annuels antérieurs³¹. Les envois par télécopieur ont également fait l'objet de commentaires du Comité permanent des opérations gouvernementales³². Le GTNO a déjà indiqué qu'il souhaite réduire l'utilisation des télécopieurs dans la prestation des services de santé et des services sociaux dans la dernière décennie et qu'il « est en train d'élaborer un plan qui permettra de mieux comprendre l'utilisation qui est faite des télécopieurs à l'heure actuelle dans le système de santé et des services sociaux des TNO et de continuer de déployer des efforts pour réduire encore l'utilisation des télécopieurs »³³.

En 2022, l'ASTNO a créé une politique sur l'envoi par télécopieur de renseignements sur les patients s'appliquant à l'ensemble du réseau. Cette politique prévoit que « seuls les renseignements urgents pour la continuité des soins aux patients doivent être transmis par télécopieur ». Il s'agit d'une restriction utile sur l'utilisation des télécopieurs; toutefois, la même restriction figure dans la politique antérieure de 2011³⁴. Les deux politiques comportent des différences, mais aussi de nombreuses similitudes. Il reste à voir si une nouvelle politique aura un effet significatif sur la fréquence des cas d'atteinte à la vie privée.

Le CIPVP continuera de surveiller cette question.

³¹Vous 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>

³²https://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.

³³Tiré 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

³⁴Politique sur la transmission par télécopieur de renseignements sur les patients de l'Administration de santé territoriale Stanton, datée de janvier 2011.

Recommandation 6 : *Les dépositaires de renseignements médicaux devraient continuer à réduire ou éliminer l'utilisation de télécopieurs pour transmettre des renseignements médicaux personnels.*

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. Une divulgation non autorisée peut facilement se produire si un employé envoie des renseignements personnels sur la santé dans un courriel à la mauvaise adresse électronique ou au mauvais groupe de destinataires, ou s'il joint les mauvais documents à un courriel. Des courriels qui auraient dû être adressés à un seul destinataire ont été envoyés par erreur à un grand nombre de personnes en utilisant la fonction « c. c. » au lieu de la fonction « c. c. i. ». 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. Ces mesures de sécurité sont déjà définies dans une certaine mesure dans la Politique sur les renseignements stockés et transférés à l'aide de moyens électroniques. Comme mentionné précédemment, une formation adéquate sur la protection de la vie privée est essentielle pour veiller à ce que les employés connaissent les mesures de protection applicables.

Recommandation 7 : *Les dépositaires de renseignements médicaux devraient utiliser des moyens de transmission électronique sécurisée lorsqu'ils envoient des renseignements médicaux personnels.*

Formation sur la protection des renseignements personnels

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. La formation sur les politiques et procédures de protection de la vie privée est primordiale pour créer une culture de protection de la vie privée sur le lieu de travail.

Le ministère de la Santé et des Services sociaux (MSSS) a créé en 2017 la Politique sur la formation obligatoire, exigeant qu'une formation en matière de protection des renseignements personnels soit 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. L'objectif de la Politique sur la formation obligatoire est de 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.

Le fait que des employés occupent des postes sans avoir reçu une formation adéquate en matière de protection de la vie privée et que la direction ne documente pas correctement les formations demeure un problème. 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 adéquate du personnel exige des ressources et un soutien permanent de la part de la direction.

Recommandation 8 : *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.*

Évaluations des répercussions sur la vie privée

Cette année, le Commissariat a examiné neuf évaluations des répercussions sur la vie privée (ÉRVP) soumises par le MSSS et l'ASTNO, pour ensuite formuler des commentaires. Plusieurs des ÉRVP concernaient des systèmes de gestion et de communication de renseignements médicaux censés appuyer la réaction du gouvernement à la pandémie de COVID-19.

La *Loi sur les renseignements sur la santé* exige que l'on réalise une ÉRVP pour déterminer les risques possibles d'atteinte à la vie privée posés par les nouveaux systèmes de communication des renseignements médicaux et par les changements qu'on y apporte³⁵. La Loi permet également au commissaire de formuler des commentaires sur les ÉRVP³⁶, vraisemblablement pour que le dépositaire de renseignements médicaux puisse en tenir compte 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 d'un projet, puisque plus tard, d'autres considérations (p. ex., temps ou coûts associés à une reprise de la conception) peuvent compliquer l'adoption de modifications visant à améliorer les mesures de protection des renseignements personnels. Il faut effectuer une ÉRVP bien avant la mise en œuvre d'un projet et surtout avant que tout renseignement médical personnel soit intégré dans le système ou utilisé de manière opérationnelle.

Ces documents prennent beaucoup de temps à préparer, tout comme l'examen d'une ÉRVP; il ne s'agit pas que de cocher des cases. Certaines ÉRVP parviennent au Commissariat quelques jours seulement avant la date prévue de mise en place du projet ou du système en question. Avec de tels délais, nous pouvons remarquer que l'examen des ÉRVP par le Commissariat est vu comme un exercice effectué à la conclusion d'un projet pour la forme, plutôt que comme une partie intégrante des premières phases de planification et de conception.

Bien que des ÉRVP soient soumises, il faudra déployer plus d'efforts pour qu'elles soient utiles dans le cadre de la conception d'un projet. Malheureusement, la Loi ne précise pas à quel moment il faut remplir une ÉRVP et la soumettre au commissaire, ou même s'il est nécessaire de tenir compte des commentaires du commissaire. D'un point de vue pratique, cependant, l'ÉRVP doit être remplie et transmise aux fins d'examen et de commentaires au début de l'élaboration d'un projet afin que tout commentaire du commissaire puisse être pris en compte et incorporé

³⁵Article 89

³⁶Article 175

à la conception du projet, s'il y a lieu³⁷. Notons que les modifications apportées à la *Loi sur l'accès à l'information et la protection de la vie privée* visent expressément ces exigences relatives aux ÉRVP³⁸.

Recommandation 9 : Une évaluation des répercussions sur la vie privée devrait être remplie et soumise pour tout nouveau système d'information ou toute nouvelle technologie de communication qui implique la collecte, l'utilisation ou la divulgation de renseignements médicaux personnels de sorte à donner un délai raisonnable pour l'examen par le commissaire à l'information et à la protection de la vie privée et pour la prise en compte des commentaires du commissaire par le dépositaire de renseignements médicaux lors des étapes de planification avant la mise en œuvre.

Recommandation 10 : L'Assemblée législative devrait envisager de modifier l'article 89 de la Loi sur les renseignements sur la santé afin d'inclure des dispositions relatives aux évaluations des répercussions sur la vie privée semblables à celles prévues à l'article 42.1 de la Loi sur l'accès à l'information et la protection de la vie privée.



Activités intergouvernementales

Les commissaires à l'information et à la protection de la vie privée du gouvernement fédéral et des provinces et territoires poursuivent leurs rencontres régulières en ligne pour communiquer de l'information, participer à des présentations et discuter des politiques, de la technologie, des propositions législatives et de divers autres sujets et questions liés à l'accès à l'information et à la protection des renseignements personnels. Ces réunions sont d'une aide précieuse pour rester informé de l'élaboration des politiques nationales et internationales.

³⁷ Cela 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_privée.pdf

³⁸ Voir l'article 42.1 de la *Loi sur l'accès à l'information et la protection de la vie privée*.

La conférence annuelle des commissaires à l'information et à la protection de la vie privée s'est tenue en personne à St. John's, à Terre-Neuve-et-Labrador, en septembre 2022. En plus de transmettre des rapports gouvernementaux et de participer à de nombreuses présentations sur des questions émergentes, la conférence a permis de conclure une résolution concernant l'obtention de la confiance du public dans les services de santé numériques. La résolution peut être consultée à l'adresse suivante : https://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_220921/.

La deuxième conférence annuelle des enquêteurs s'est déroulée en ligne en novembre 2022. Le commissaire adjoint et l'enquêteur du Commissariat ont tous deux participé à cette réunion enrichissante axée tant sur les compétences que sur les connaissances. De l'avis général, l'expérience a été bénéfique, et le Commissariat participera de nouveau à la conférence cette année.

Dernières réflexions

Le droit à la vie privée, soit le droit d'être laissé en paix, de ne pas subir d'intrusion ou d'ingérence de la part d'autres personnes, y compris de l'État, est un droit fondamental qui trouve son fondement constitutionnel dans l'article 8 de la *Charte canadienne des droits et libertés*. La *Loi sur l'accès à l'information et la protection de la vie privée* et la *Loi sur les renseignements sur la santé* prévoient des mesures particulières de protection de la vie privée en ce qui concerne les renseignements personnels détenus par nos institutions publiques.

Lorsque les gouvernements fournissent des services aux individus, des renseignements personnels sont inévitablement collectés, utilisés et parfois divulgués. Tandis que les services publics se numérisent de plus en plus, la collecte électronique de renseignements personnels, qui est déjà considérable, continuera de prendre de l'importance. La création, l'utilisation et le stockage de données électroniques permettent aux gouvernements de réaliser des gains d'efficacité considérables dans la fourniture de services aux citoyens. Je ne suis pas le seul à aimer la commodité de renouveler mon permis de conduire et l'immatriculation de mon véhicule en cliquant sur quelques boutons plutôt qu'en faisant la queue à un bureau d'enregistrement.

Cependant, ces gains s'accompagnent souvent d'une augmentation des risques d'utilisation ou de divulgation non autorisée. Les ensembles de données personnelles peuvent être ciblés par des individus malveillants qui utilisent des rançongiciels ou commettent des usurpations d'identité, et les administrations publiques en sont souvent victimes. Les gouvernements doivent surveiller l'environnement de risque et protéger les systèmes électroniques contenant des renseignements personnels au moyen de mesures de sécurité raisonnables, c'est-à-dire la conception de systèmes de protection de la vie privée, le cryptage, les mots de passe, les réseaux privés virtuels, les protocoles de transfert de fichiers sécurisés, la formation des utilisateurs, les politiques et les procédures de protection de la vie privée, les audits réguliers, la surveillance, etc. Une bonne protection de la vie privée exige des efforts considérables!

De nouvelles menaces émergent. Nombreux sont ceux qui soulèvent des préoccupations quant à l'« intelligence artificielle », qu'ils considèrent comme une menace pour la vie privée ainsi

qu'une menace existentielle. Alors que les menaces potentielles pour la vie privée continuent de se multiplier et deviennent de plus en plus sophistiquées, les efforts et les ressources nécessaires pour les contrer doivent également être décuplés. Le gouvernement des Territoires du Nord-Ouest n'a pas subi de cyberattaque majeure, telle que celles lancées contre le gouvernement du Nunavut en 2019 et contre le système de santé du gouvernement de Terre-Neuve-et-Labrador en 2021, mais la menace potentielle est bien présente. Chaque organisme public et chaque dépositaire de renseignements médicaux doit évaluer ses mesures de sécurité et assurer une défense solide pour protéger les renseignements personnels dont il a la charge et le contrôle.

Il est juste d'observer que des couches supplémentaires de sécurité peuvent réduire les gains d'efficacité potentiels. Parfois, les mesures de sécurité comme les mots de passe peuvent être perçues comme des obstacles à l'efficacité, du moins jusqu'à ce qu'une atteinte à la vie privée survienne. Lors d'un examen réalisé cette année³⁹, j'ai appris qu'un organisme public avait stocké un nombre important de dossiers d'employés dans le système intégré de gestion de l'information numérique (DIIMS) sans établir un mot de passe ou d'autres contrôles de sécurité appropriés. Des employés non autorisés ont pu accéder librement aux dossiers pendant une longue période. L'intervention de l'organisme a nécessité des efforts importants et coûteux; plusieurs employés ont consacré des mois à la gestion de l'atteinte. Cette situation constitue un exemple instructif dont les organismes publics doivent tenir compte lorsqu'ils décident des ressources à consacrer aux mesures de protection de la vie privée. Les implications d'une atteinte à la vie privée, tant sur le plan financier qu'en matière de ressources humaines, peuvent être considérables!

À l'avenir, je recommande vivement aux organismes publics de veiller à mettre en place des mesures de sécurité raisonnables et efficaces afin de protéger les renseignements personnels qui leur sont confiés. Une vigilance constante est essentielle.

Enfin, c'est avec une grande tristesse que nous soulignons le décès de M^{me} Elaine Keenan Bengts le 8 août 2022. Après une longue carrière juridique qui l'a amenée à servir les Territoires du Nord-Ouest et le Nunavut en tant que première commissaire à l'information et à la protection de la vie privée de 1997 à 2020, M^{me} Keenan Bengts a vu ses projets de retraite bien méritée écourtés par la maladie. Elle était animée d'une passion inspirante et infatigable pour le travail accompli par le Commissariat et a beaucoup apporté à la population des Territoires du Nord-Ouest. Elle nous manquera énormément.



³⁹Tiré du document suivant (en anglais) : *Applicant A (Re)*, 2022 NTIPC 20 (CanLII), <https://canlii.ca/t/jtpkw>

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 devraient revoir leurs obligations légales de répondre aux demandes d'accès à l'information et évaluer leur capacité à fournir des réponses dans les délais impartis par la loi. Ils doivent également veiller, collectivement ou individuellement, à ce que le BAIPVP dispose de ressources suffisantes pour fournir une assistance fiable aux organismes publics afin qu'ils répondent aux demandes d'accès à l'information dans les délais légaux et se conforment aux exigences procédurales appropriées. (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 ministère de la Santé et des Services sociaux 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 qu'ils informent le commissaire de la mise en œuvre des recommandations acceptées. (Page 16)*

Recommandation 5 : *Le GTNO devrait examiner la nécessité d'adopter des politiques et des procédures de protection de la vie privée pour soutenir un groupe d'intervention spécialisée en cas d'urgence, comme le Secrétariat de coordination pour la COVID-19, et s'assurer qu'il est équipé pour mener ses activités dans les limites de la Loi sur les renseignements sur la santé. (Page 18)*

Recommandation 6 : *Les dépositaires de renseignements médicaux devraient continuer à réduire ou éliminer l'utilisation de télécopieurs pour transmettre des renseignements médicaux personnels. (Page 20)*

Recommandation 7 : *Les dépositaires de renseignements médicaux devraient utiliser des moyens de transmission électronique sécurisée lorsqu'ils envoient des renseignements médicaux personnels. (Page 20)*

Recommandation 8 : *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 21)*

Recommandation 9 : *Une évaluation des répercussions sur la vie privée devrait être remplie et soumise pour tout nouveau système d'information ou toute nouvelle technologie de communication qui implique la collecte, l'utilisation ou la divulgation de renseignements médicaux personnels de sorte à donner un délai raisonnable pour l'examen par le commissaire à l'information et à la protection de la vie privée et pour la prise en compte des commentaires du commissaire par le dépositaire de renseignements médicaux lors des étapes de planification avant la mise en œuvre. (Page 22)*

Recommandation 10 : *L'Assemblée législative devrait envisager de modifier l'article 89 de la Loi sur les renseignements sur la santé afin d'inclure des dispositions relatives aux évaluations des répercussions sur la vie privée semblables à celles prévues à l'article 42.1 de la Loi sur l'accès à l'information et la protection de la vie privée. (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.**