TD 481-19(2) TABLED ON NOVEMBER 24, 2021

Northwest Territories

20/21

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NORTHWEST TERRITORIES

# Annual Report

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

---

Kīspin ki nitawihtīn ē nīhīyawihk ōma ācimōwin, tipwāsinān.
Cree

---

Tłı̨chǫ yatı k'ǫ̀ǫ́ Dı wegodı newǫ dè, gots'o gonede.
Tłı̨chǫ

---

ʔerıhtł'ís Dëne Sųłıné yatı t'a huts'elkër xa beyáyatı theɔą ɔat'e, nuwe ts'ën yółtı.
Chipewyan

---

Edı gondı dehgáh got'ı̨e zhatıé k'ǫ́ǫ́ edatł'éh enahddhę nıde naxets'ę́ edahłí.
South Slavey

---

K'áhshó got'ı̨ne xədə k'é hederı ɔedı̨htl'é yerınıwę nídé dúle.
North Slavey

---

Jii gwandak izhii ginjìk vat'atr'ijąhch'uu zhit yinohthan jì', diits'àt ginohkhìi.
Gwich'in

---

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.
Inuvialuktun

---

ᑖᒃᑯᐊ ᑎᑎᖅᑲᐃᑦ ᐱᓕᒍᐁᐱᑦ ᐃᓄᒃᑎᑐᓪᓗᖅᓯᒪᓕᓂᑎᒃ, ᐅᖃᖅᑎᖅᓄᑦ ᐅᖅᑰᓕᕐᓇᖅᑐᑎᑦ.
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*

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

July 1, 2021

The Hon. 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, 2020, to March 31, 2021.

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@atipp-nt.ca

# Table of Contents

# Commissioner's Message

I am pleased to present this Annual Report for the period April 1, 2020, to March 31, 2021, my first since being appointed as the Information and Privacy Commissioner on November 23, 2020.

I would like first to recognize my predecessor, Elaine Keenan Bengts, who served as the Commissioner continuously since the creation of the office in 1997. Ms. Keenan Bengts' tireless work over many years has created an effective, widely respected office with a dedicated and enthusiastic staff. Her legacy of published Review Reports has already been and will continue to be a valuable resource for applying and understanding our legislation.

As with many workplaces, the COVID-19 pandemic affected the Office of the Information and Privacy Commissioner (OIPC). With some adjustments the OIPC was able to shift to working remotely from home. In the main, work proceeded without much delay. This was essential: there was no statutory relief from the timelines in the *Access to Information and Protection of Privacy Act* (*ATIPPA*) or the *Health Information Act* (*HIA*), either for government departments or the Information and Privacy Commissioner. Several statutory timelines were abridged by statute in 2020, but none involving these two *Acts*: a clear indication from the legislature that keeping the operations of government open and transparent is a priority!

The public's exercise of the right to access government information appears to be increasing. With some concern, I note that my office received a number of requests for review this year regarding the timeliness of some responses to access to information requests. While public bodies have pointed to the pandemic as a reason for delay, the other challenge identified is the number and scope of other access to information requests the public bodies are dealing with. Greater use of the access to information 'machinery' suggests a greater public interest in the activities of government. Of course, greater use also requires monitoring by government to ensure sufficient resources are in place to enable public bodies to respond to access requests appropriately.

The use of fax machines to transmit personal health information continues to be a source of privacy breaches under the *HIA*. The use of email to communicate personal information or personal health information has also led to a number privacy breaches. Although the number of privacy breaches reported to the Commissioner has not abated from previous years, I am nevertheless optimistic. In reviewing privacy breach reports provided under the *HIA,* my office has observed real improvement of public bodies' awareness of privacy issues and best practices for appropriate handling of personal information and personal health information.

Having effective privacy protection policies and procedures in place is essential, and it is evident that public bodies are making efforts to ensure these are in place when deficiencies or issues are identified by this office. Ensuring that employees are well trained in those policies and procedures and in the proper use of technology will be an on-going task for health information custodians under the *HIA* and for public bodies under the *ATTIPA*. With increased awareness of

those policies and procedures, and continued investment in privacy training for employees, positive changes can be made to public bodies' ability to respect and protect individuals' privacy.

Individuals may request the Commissioner to review whether a public body has collected, used, or disclosed personal information in contravention of the *ATIPPA* or *Health Information Act*. The *HIA* requires notice to an individual of an unauthorized use or disclosure of personal health information. Currently there is no similar requirement under the *ATIPPA* but amendments to the *ATIPPA* will require public bodies to report 'material' breaches of privacy to the Commissioner and to notify individuals where it is reasonable to believe that the breach creates a 'real risk of significant harm.' In comparison, the *HIA* requires notice to the Commissioner and individuals for all unauthorized disclosures of personal health information. The threshold for breach reporting under the *HIA* may result in more notifications, but it also ensures individuals are made aware of how their personal health information is being managed, and it provides potentially more effective oversight by bringing 'minor' privacy breaches under scrutiny so they can be addressed, thereby helping avoid future events that may cause greater harm. While some public bodies already report privacy breaches to my office, after the amendments come into force, we expect to see an increase in the number of privacy breach notifications. How public bodies apply the different notification thresholds will likely come under scrutiny as and when breaches may occur, and we will be monitoring this issue closely.

Oversight of public bodies and health information custodians is essential to ensure personal privacy is protected and to assure the public that the government is taking appropriate measures to that end. Being proactive and having effective governance with appropriate privacy policies and records handling procedures in place are each critical to protecting individuals' privacy. Ensuring employees are properly trained and have the necessary knowledge, skills and suitable technology is also fundamental to privacy protection. We recognize that providing these privacy safeguards is a challenge anywhere and can be harder still with a geographically dispersed and ever-changing workforce.

While the OIPC and the public bodies prepare for the changes required by the *ATIPPA* amendments, the independent oversight provided by my office will assist public bodies to keep focused on the fundamental purposes of the legislation: the right of the public to access government records and the protection of personal privacy. While the government works to deliver services and to help the citizens of the Northwest Territories emerge from the pandemic, it must also ensure these rights are well protected. The future looks busy; I look forward to the work ahead.

# Financial Report

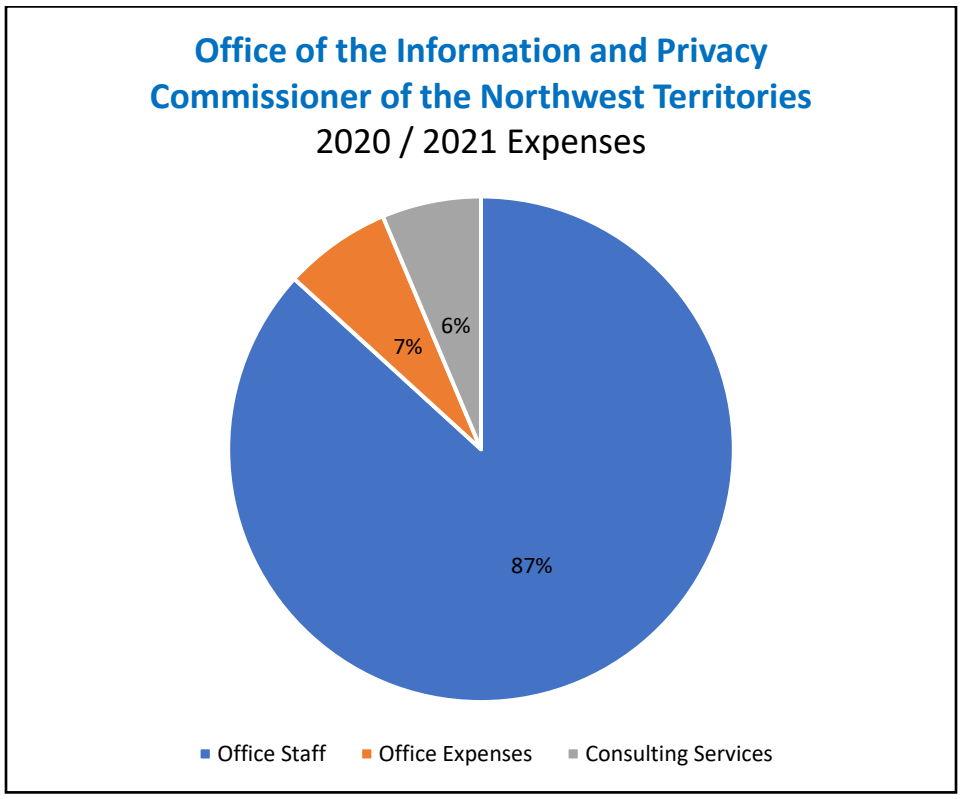
The total amount spent to operate the Office of the Information and Privacy Commissioner (OIPC) of the Northwest Territories for the fiscal year 2020/2021 was $547,168.63. A detailed breakdown is outlined in the charts on the next page.[1]

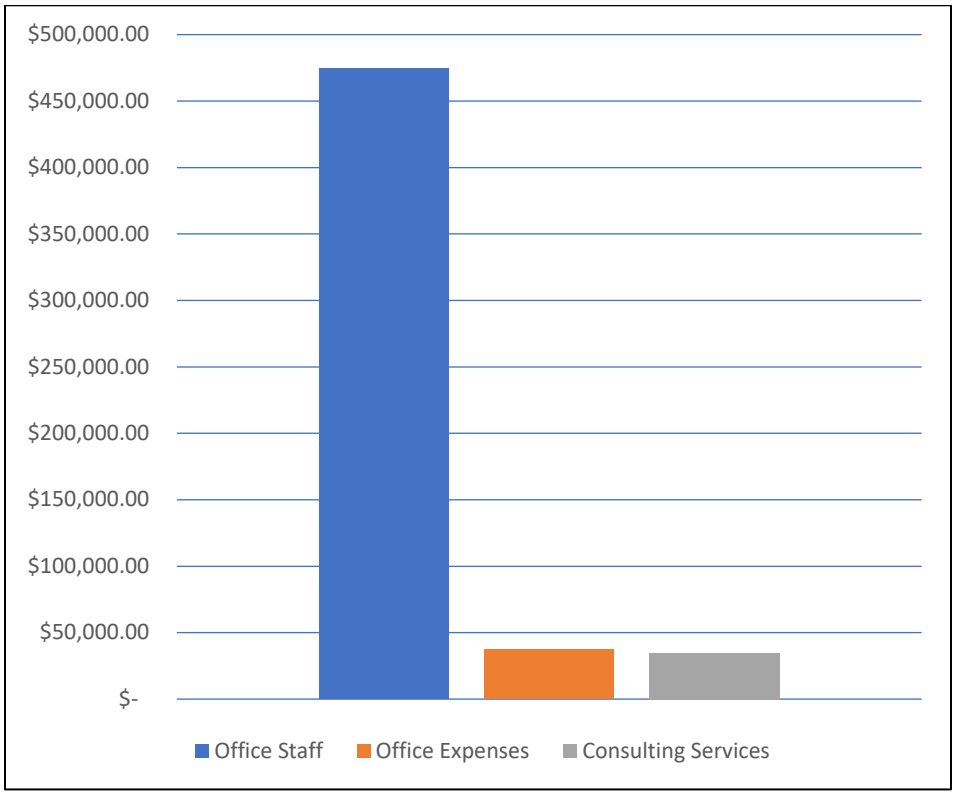
New computer hardware and software were installed in December of 2020. This immediately improved the utility and stability of the office systems. The OIPC is most grateful to the former Commissioner, Ms. Keenan Bengts, who prioritized this improvement! It has been of great assistance to all, both in the office and during a period of remote work earlier this year.

The workload for the OIPC has steadily increased in recent years and this trend continues. As a point of comparison, at the end of the first quarter last year this office had opened 82 files; for the same period this year, we have opened 112 files. To address this situation, last year the Legislative Assembly approved additional annual funding to add an Investigator position. The hiring process is underway and when completed the OIPC cohort will increase from three to four.

Whether this staffing level will be sufficient as we move forward remains to be seen. There is a significant file backlog and the increase in file numbers over previous years suggests an increasing demand for this office's services. Of course, the mandate of the OIPC extends beyond conducting reviews, and the general powers of the Commissioner under section 67 of *ATIPPA* were expanded in the amendments; however, our capacity for activities such as public education and other communication functions remains quite limited. A 2019 review of the OIPC functions identified a need for more staff for these additional functions, the Commissioner will monitor this situation over the next year and explore opportunities for meeting all the office's responsibilities.

[1] Due to the pandemic, no travel expenses were incurred this year.


Office of the Information and Privacy Commissioner of the Northwest Territories
2020 / 2021 Expenses
6%
7%
87%
Office Staff
Office Expenses
Consulting Services


$500,000.00
$450,000.00
$400,000.00
$350,000.00
$300,000.00
$250,000.00
$200,000.00
$150,000.00
$100,000.00
$50,000.00
$-
Office Staff
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 (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*. The *ATIPP Act* enshrines four key rights and obligations:

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

The *Act* outlines the process for members of the public to obtain access to records and it establishes when and how public bodies can collect, use, or disclose personal information about individuals. Independent review of public bodies' decisions and actions is provided by the Commissioner.

## The *Health Information Act*

The *Health Information Act* (*HIA*) governs the collection, use and disclosure of personal health information, recognizing both the right of individuals to access and protect their personal health information and the need of health information custodians to collect, use and disclose personal health information to support, manage and provide health care. The legislation 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 Tłı̨chǫ Community Services Agency, and private physicians and pharmacies operating in the Northwest Territories.

The *HIA* sets out the rules for health service providers regarding the collection, use and disclosure of personal health information and establishes the duty for health information

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

The *HIA* also requires health information custodians to notify affected individuals if personal health information is used or disclosed other than as permitted by the *Act*, or if it is stolen, lost, altered, or improperly destroyed. Notice to the Commissioner is required in the event of an unauthorized disclosure, or in the event of unauthorized use, loss, or destruction where there is a reasonable risk of harm. In such circumstances, the Commissioner may conduct an investigation and prepare a report with appropriate recommendations for the consideration of the health information custodian.

## The Information and Privacy Commissioner

The Information and Privacy Commissioner is appointed on the recommendation of the Legislative Assembly. The Commissioner reports directly to the Legislative Assembly of the Northwest Territories and is independent of the government.

Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner carries out the duties and functions set out in the *Access to Information and Protection of Privacy Act (ATIPPA)* and the *Health Information Act (HIA)*. The OIPC provides independent review of decisions made by public bodies and health information custodians when responding to access to information requests and investigates allegations of privacy breaches under the *ATIPPA* and the *HIA.* If a public body's response to an access to information request, or a request for correction of personal information, does not satisfy the applicant, the applicant may request a review by the Information and Privacy Commissioner. Similarly, where an individual believes their personal information or personal health information has been collected, used, or disclosed without legal authority, the individual may request a review by the Information and Privacy Commissioner. In some situations, the Commissioner may conduct a review on his own initiative.

Public access to government records and protection of individuals' personal information are essential to create transparency and trustworthiness of government, both of which are vital for effective democracy. Access to government records is an important legal right, though it is not unfettered: there are specific statutory exceptions – some mandatory, some discretionary – that permit public bodies to withhold records. When public bodies decide what records to disclose in response to an access to information request, the issues that can arise are numerous and can be complex. Independent oversight helps ensure public bodies comply with legislation and can help assure individual applicants that their rights are being upheld.

The Commissioner investigates complaints by first obtaining input from the parties concerned. In some cases, an informal early resolution of the matter may be possible; frequently, matters will proceed further. After determining the facts and receiving any representations from the applicant, the public body, and any third parties, and after applying the relevant sections of the legislation, the Commissioner will issue a report which may make recommendations to the public body or health information custodian.

Public bodies and health information custodians are not currently required to accept the Commissioner's recommendations, but the Commissioner's Annual Reports are required to report where a public body decides not to follow a recommendation. Applicants who are unsatisfied with a public body's decision regarding a recommendation may appeal the decision to the Supreme Court of the Northwest Territories.

When the amendments to the *ATIPPA* come into force the role of the Information and Privacy Commissioner will change: the power to make recommendations will become a power to make binding orders which may be filed in the Supreme Court of the Northwest Territories and enforced as an order of the Court. A Commissioner's order may be appealed to the Supreme Court of the Northwest Territories. This order-making power will not apply to matters under the *HIA*: the Commissioner will continue to make recommendations under that *Act*.

In addition to dealing with complaints, the Commissioner also reviews and comments on the privacy protection implications of proposed legislation or government policies or programs, and this will often include review and comment on Privacy Impact Assessments. Privacy Impact Assessments are currently required under government-wide policy and under the *HIA* and will be required in some circumstances under the amendments to the *ATIPPA*.

# The Year in Review

The Office of the Information and Privacy Commissioner opened a total of 162 files in the fiscal year 2020/2021. Of that total, 75 were Access to Information and Protection of Privacy files and the remaining 87 were Health Information files.

## *Access to Information and Protection of Privacy Act*

The OIPC opened 75 files under the *Access to Information and Protection of Privacy Act* between April 1, 2020, and March 31, 2021:

| | |
|---|---|
| Requests for Review – Access to information | 26 |
| Requests for Review – Fees, Delays & Extension of time | 8 |
| Requests for Review – 3rd party requests | 4 |
| Consultations/Comments – Acts, legislations, bills | 8 |
| Privacy Issues – Breaches and Complaints | 26 |
| Corrections – To personal information | 1 |
| Miscellaneous & Administrative | 2 |

## *Health Information Act*

The OIPC opened 87 files under the *Health Information Act* between April 1, 2020, and March 31, 2021:

| | |
|---|---|
| Privacy Breach Notifications | 66 |
| Request for Review - Privacy Breach | 10 |
| Comments – Privacy Impact Assessments | 7 |
| Comments – Health policies, acts, processes | 3 |
| Miscellaneous & Administrative | 1 |

## Review Reports – *Access to Information and Protection of Privacy Act*

Twenty-eight Review Reports were issued under the *Access to Information and Protection of Privacy Act* (*ATIPPA*) in 2020/2021. The reports deal with reviews of responses to access to information requests under section 28 of the *ATIPPA* and with reviews of unauthorized collection, use or disclosure of personal information under section 49.1. Section 28 reviews address the sufficiency and timeliness of responses to access to information requests, and the potential impacts on the privacy of third parties whose personal information was within the scope of the access to information request. Section 49.1 reviews address whether personal information was collected, used, or disclosed without legal authorization. Reports are available on-line at https://www.canlii.org/en/nt/ntipc/ [2].

Section 68 of the *ATIPPA* requires the Annual Report to include information concerning any instances where recommendations of the Information and Privacy Commissioner made in a review were not followed. This includes instances where the public body has neglected to respond to the Commissioner's recommendations within 30 days of receipt of a Review Report, which constitutes a deemed refusal to accept the recommendations. In most instances, the public bodies did not intend to reject the recommendations and were unaware of the deeming provisions. Most of these instances were resolved through follow-up correspondence, albeit some required repeated follow-up before notice of a decision was issued.

The following are summaries of Review Reports where the public body decided not to follow the Commissioner's recommendations:

### Review Report 20-226

This was a review of a response to an access to information request made in 2019 to the Human Resources section of the Department of Finance. The response contained emails between officials discussing aspects of the applicant's employment situation. The public body made numerous redactions to the records pursuant to section 14(1) of the *Access to Information and Protection of Privacy Act*, which allows the public body discretion to refuse to disclose a record that could reasonably be expected to reveal certain types of information, such as (a) advice, proposals, recommendations, analyses, or policy options developed for a public body, or (b) consultations or deliberations involving officers or employees of a public body. The applicant sought review of the redactions made to various records.

The Information and Privacy Commissioner recommended that several parts of the records that had been redacted should be disclosed. The Department agreed to all except in regard to two paragraphs in one email. The Department continues to be of the view that the two paragraphs involve advice and should not be disclosed. The Commissioner's report provided an informative explication of section 14(1) and the types of information that the section is intended to address.

[2] Past years' decisions are also available on-line on this free public database.

The Department did not offer any further information or explanation of its decision to maintain the redaction. The Applicant was left with the bare assertion that the paragraphs contained "advice by the Department."

## Review Report 20-228

On May 27, 2019, the Applicant made an access to information request to the Department of Health and Social Services. The Department identified a total of 21 pages of responsive records but denied access to all, relying on section 23(1) of the *Access to Information and Protection of Privacy Act* and stating the disclosure of the information would result in an unreasonable invasion of an individual's privacy. In denying access, the Department identified the requested information as being information about a third party's employment, occupational and educational history and personal information relating to the hiring and management of a third party.

At the outset of the review, and at the Commissioner's suggestion, the Department disclosed the 21 pages of records to the applicant, but with significant redactions. The Department cited sections 14(1)(a) and 23(2)(d) of the *Act* as authority for the redactions. The review proceeded in regard to the records disclosed in redacted form.

During the review, the Department provided written representations to explain its application of the *Act*. The Commissioner found the Department's reasons did not meet the requirements of the *Act* and recommended that access to the records be granted with significantly less redaction. The Department decided not to follow some of the recommendations, withholding some records and citing a section of the *Act* not relied on during the review.

This is highly problematic: the *Act* does not contemplate a process whereby a public body can test the application of different sections in an iterative manner. During a review a public body has the opportunity to make full written representations so that the reasons for the initial decision to deny access to a record can be properly considered by the Commissioner. Rejecting a Commissioner's recommendation for reasons not set out in the public body's representations effectively denies the Commissioner the benefit of the public body's reasoning. This potentially denies the applicant the opportunity to have all the relevant issues addressed in the Commissioner's review. This is an important aspect of procedural fairness. Such an approach suggests a lack of diligence in providing the Commissioner with complete representations at the first instance, and it may also suggest the intention to withhold parts of a record derives from some interest other than a properly considered application of the *Act*. A public body should provide <u>all</u> the evidence and arguments on which it intends to rely when providing representations to the Commissioner during a review.

## Review Report 20-229

This report reviewed the Department of Industry, Tourism and Investment's response to an access to information request for emails and attachments regarding the applicant and the

applicant's business. The Department identified 4602 responsive records for the period specified, many of which contained duplicate emails. Most of the records were disclosed with no or minimal redaction. The Department made some redactions pursuant to section 23, which governs the protection of personal information of third parties, and pursuant to sections 14(1)(a) and (b), which permit a public body to refuse to disclose information where the disclosure could be reasonably expected to reveal advice, proposals, policy options, etc., developed for a public body or member of the Executive Council, or where disclosure would reveal consultations or deliberations involving officers or employees of a public body. The Applicant sought a review of the redactions.

The Commissioner recommended several of the redactions remain, though in some cases for different reasons than the public body provided. In some instances, the Commissioner recommended less redaction than what the public body proposed. In other instances, the Commissioner recommended the Department reconsider the redaction of some information in light of the possible application of section 24 of the *Act*, which protects certain kinds of 'business interest' information. In still other instances, the Commissioner recommended that the Department reconsider the redaction pursuant to section 14(1)(a) or (b), each of which requires the application of discretion by the public body.

Of the 39 separate recommendations to disclose more information, 36 were accepted in whole, and three were accepted in part. The Department provided explanations for maintaining some of the redactions, identifying specific concerns about the potential sensitivity of some of the information. In each case the redactions differed from the Commissioner's recommendations in regard to only a few words. The Commissioner made an additional 10 recommendations to reconsider the application of section 23 or 24 or the exercise of discretion under section 14 (1), all of which resulted in the public body disclosing further information and articulating its reasons.

## Review Report 20-230

The Department of Infrastructure responded to an access to information request for emails and attachments regarding the applicant and the applicant's business. The Commissioner provided the Review Report to the Department on May 21, 2020. The Department provided a response to the Applicant by letter dated July 2, 2020, but did not notify the Commissioner until October 2, 2020, after letters of inquiry were sent by the OIPC on July 17, 2020, and then October 1, 2020. Under section 36 of the *Act*, a public body has 30 days to notify the Commissioner of its decision regarding any recommendation.

The documents produced for the applicant were reviewed as four separate 'packages' totalling 902 pages. Package Two contained 171 pages, of which three pages -- a chart of workplace accident claims -- were extensively redacted on the basis of 'relevance.' Relevance is not a basis for non-disclosure under the *Act*. The Commissioner recommended that these three pages of redactions be reconsidered by the Department with a view to determining if any of the exceptions in sections 13 to 25 of the *Act* applied to any of the records. The Commissioner

proposed that "the organization name, accident date, WSCC registration date, claim category, late penalty and location are all data points that could be disclosed without resulting in an unreasonable invasion of privacy." The Department decided to disclose most of the information in these three pages excepting only the individuals' locations to ensure that no third parties were identifiable. This recommendation applied to three similar charts in Package Two as well. Other than not disclosing the location of the claimants, virtually all of the Commissioner's recommendations were accepted.

## Review Reports - *Health Information Act*

Fourteen Review Reports were issued under the *Health Information Act* in 2020/2021. 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/ . The reports review various instances of unauthorized collection, use or disclosure of personal health information.

In some instances, an individual's personal information was incorrectly identified in paper or electronic records or disclosed to the wrong individuals. Not infrequently, personal health information has been unlawfully disclosed when using fax machines to transmit personal health information. This has been the subject of comment by the Commissioner in past years' Annual Reports, and more recently in reports 20-HIA 26 and 20-HIA 27 this year. While the health information custodians have committed to decreasing the use of fax communication in the delivery of health services, mistakes related to the use of fax machines continue to generate reports about mismanaged fax machines, misdirected faxes, gaps in relevant training, and other issues resulting in the unlawful disclosure of personal health information.

Personal health information is inherently sensitive, and privacy breaches regarding personal health information is always of concern. One particularly significant event occurred in July 2019: patient records from the old Stanton Territorial Hospital were found by a private individual at the Yellowknife solid waste facility. Compact discs with patient identification were found alongside other materials from the decommissioned hospital. After conducting a preliminary investigation, the NTHSSA hired independent investigators to conduct a formal investigation. Unfortunately, the investigation was hampered because staff at the waste facility had gathered the materials and baled and buried them before investigators attended the scene. While this likely minimized any further potential breach of privacy it also made it challenging to identify the individuals of concern and to determine the details of the personal health information involved. The Commissioner received the NTHSSA's investigation report and the evidence binder, although there were some parts of some pages missing from the report and there were a small number of redactions. The Commissioner's report 20-HIA 31 addressed a series of issues regarding the circumstances that led to the breach, and regarding the response to the breach. These issues included various aspects of records storage and transfer, the use and training of contractors when handling personal health information, methods to minimize risk and mitigate any unlawful disclosure of personal health information, multi-department project planning and coordination,

destruction of evidence, lack of timeliness in breach reporting to NTHSSA, lack of coordination of activities and actors during the hospital move, and others. The Commissioner proposed 27 separate recommendations. NTHSSA accepted all in its letter dated May 29, 2020.

Section 173(b) of the *Health Information Act* requires the Commissioner's Annual Report to include information regarding any recommendations made as part of a review that were not followed by the health information custodian. The following are summaries of Review Reports where the health information custodian decided not to follow the Commissioner's recommendations:

### Review Report 20-HIA 24

This review addressed an instance where a locum physician – a physician hired on a temporary basis, often from another province or territory – accessed a patient's medical record without permission and for a purpose not connected with that patient's care or otherwise permitted by law. The physician accessed Patient B's record in the electronic medical record system (EMR) during an appointment with Patient A, purportedly in aid of an assessment of Patient A's medical situation. The physician noted some details of Patient B's personal health information in Patient A's EMR record. Patient B was not aware of and did not consent to the accessing or disclosure of this personal health information. There was no legal justification for the physician to access Patient B's records. The physician claimed that this type of access to a third party's medical records was common practice in the physician's home jurisdiction, but the College of Physicians and Surgeons from that province confirmed the opposite.

There were additional issues identified during the Commissioner's investigation. First, the breach occurred in June 2018 but was not reported to the Commissioner or Patient B until April 2019 – a nine-month delay -- even though the breach was discovered by another health practitioner shortly after the incident occurred. Second, the information included in the breach notices to the individual and the OIPC were lacked sufficient detail to understand the nature of the breach. Third, the health information custodian -- Northwest Territories Health and Social Services Authority (NTHSSA) – resisted the idea of removing the reference to Patient B's information from Patient A's medical records despite this being an instance of an unlawful use of Patient B's personal health information.

The Information and Privacy Commissioner made seven recommendations to address the situation. These addressed the following:

(a) Possible disciplinary measures for the physician as may be required by NTHSSA by-laws, *Health Information Act* regulations, and section 185 of the *HIA* which makes it an offence to knowingly collect, use or disclose personal health information in contravention of the *Act*.

(b) The need to ensure and to document that all staff, including locum physicians, complete appropriate privacy training before providing health services and handling personal health information;
(c) The removal of the notations regarding Patient B's personal health information from Patient A's records and making a notation in Patient B's records that this disclosure occurred;
(d) The need for breach notifications to individuals and to the OIPC to be timely, detailed and accurate;

NTHSSA did not accept the recommendations regarding physician discipline or the amendment of the patients' medical records. The latter was expressly subject to 'pending legal advice,' suggesting that the matter would be given further consideration. NTHSSA elaborated on its decision regarding possible discipline, saying that it would "follow current process in place outlined in the NWT Medical Bylaws to ensure any concerns regarding a physician are investigated and necessary action taken."

### Review Report 20-HIA 28

In August 2019, the Department of Health and Social Services notified the OIPC that an employee of the department had mistakenly sent a patient's relative a copy of certain personal health information (PHI) related to the patient's medical travel request. The PHI was sent intentionally; the employee did not realize at the time that this was not appropriate. The employee was acting temporarily in a position without proper knowledge or training. Before sending the information, the employee had consulted the correct program manual and asked a co-worker for advice. Neither the employee nor the co-worker sought guidance from the unit manager. The PHI that was disclosed included personal contact information, personal health care number, and the medical purpose for the travel.

Although the mistake was identified almost immediately, and by more than one staff member, the initial notification of the breach was delayed as no one at the time recognized that the disclosure to the patient's relative was not authorized under the *Health Information Act*. The Review Report examined the potential causes of the breach, the privacy safeguards in place, and the Department's response to the breach. It discussed the need for both privacy training and privacy breach response training and made observations about the risk of unauthorized disclosure of PHI inherent in the medical travel forms being used.

The Commissioner made eight recommendations to the Department in addressing different aspects of this privacy breach with a view to preventing other breaches of this kind in the future. The Review Report was submitted to the Minister by letter dated May 11, 2020. Follow-up letters seeking a response from the Minister were sent June 24, 2020, August 12, 2020. In September there was an email exchange from the Department acknowledging the delay and indicating a response was forthcoming in two to three weeks' time. The Information and Privacy

Commissioner sent further follow-up reminders on October 1, 2020, and lastly November 12, 2020.

If the health care custodian fails to communicate notice of a decision regarding the Commissioner's recommendations within 30 days of receipt of a Review Report, section 156(2) of the *Health Information Act* deems this to be a decision *not* to follow the recommendations. On June 30, 2021, fully one year after the Minister's decision was required, my office received a notice of decision from the Department accepting all eight recommendations. The delay was attributed in large part to competing priorities related to the pandemic response. As mentioned above, the legislature provided no relief from the timelines in the *HIA* despite challenges posed by the pandemic.

### Review Report 20-HIA 30

On March 21, 2019, an NTHSSA employee discovered papers with personal information and personal health information of 109 individuals in a staff house in a small community. The house had been occupied at different times by various NTHSSA staff during 2017 and 2018. The papers had been abandoned and left unsecured. Each employee had left some documents there. The house had been broken into in December 2018 and may have been occupied for a short time by persons unknown. Whether any third parties read or removed any of the documents is not known. The NTHSSA's investigation identified, among other things, a lack of knowledge and training of local employees in regard to privacy protection and records management.

Following receipt of notice from NTHSSA of the privacy breach, the Commissioner conducted a review of the incident pursuant to section 137 of the *HIA*. The Commissioner identified a few additional issues of concern, including delayed and inadequate notice to the individuals whose privacy had been breached, and an unreasonable delay in providing the Commissioner with the NTHSSA's final investigation report. The Commissioner also noted that more detail in the description of the records would have been helpful to determine the sensitivity of the information and the appropriate mode to secure such information.

During the review it became apparent that NTHSSA's investigation did not focus primarily on the privacy breach aspects. There were, no doubt, other considerations that NTHSSA was concerned with, but these need not and should not have detracted from the objective of conducting a full, detailed privacy breach investigation as contemplated by the Privacy Breach Policy (2017). Other legal or policy requirements do not supplant or displace the requirement for a thorough privacy investigation, which is essential to understand the severity of the breach and to ensure appropriate measures are taken to prevent a future recurrence.

The Commissioner made eight recommendations in the July 21, 2020, report; three were not accepted.

Recommendation #5 suggested that NTHSSA develop an investigation plan for cases involving potential breaches of both personal health information and other personal information. NTHSSA

did not accept this recommendation initially but said it was to be reviewed upon further clarification. In a follow-up letter dated November 5, 2020, NTHSSA said it would share the recommendation with the Organizational Quality Risk Management Committee, which involves both the NTHSSA and the Department of Health and Social Services. In a letter dated April 27, 2021, the NTHSSA indicated it had drafted a privacy breach policy to address both *Health Information Act* and *Access to Information and Protection of Privacy Act* breaches. It is not entirely clear how this policy aligns with the existing Department of Health and Social Services' Privacy Breach Policy,[3] but it appears that NTHSSA has now accepted the recommendation, at least in part.

Recommendation #6 proposed that NTHSSA ensure that it supplies the Commissioner upon request with all information the Commissioner may require for the purposes of any *HIA* breach investigation. NTHSSA initially decided not to accept this recommendation but to refer it to the Department of Justice for input. Later, in its November 5, 2020, letter NTHSSA referred to development of a Privacy Breach Policy. In its April 27, 2021, letter, the NTHSSA advised that it has implemented a new tracking tool that will ensure reporting and responding to the Commissioner is completed expeditiously.

While this tracking tool will undoubtedly be helpful, the recommendation was directed not to the timeliness of the responses but to their completeness. During the Commissioner's review the NTHSSA objected to producing an unredacted copy of its final investigation report to the Commissioner. This was inappropriate: section 154 of the *Act* gives the Commissioner the power to compel production of documents; as well, the *Health Information Act* guide produced by the Department directs that:

> Custodians must produce any records the Commissioner needs. These must be produced within 14 days. The Commissioner can view records (for example, on electronic health information systems) if copies cannot be produced within 14 days. The Commissioner can require any evidence to be submitted and does not have to stick to the rules of court. No one can withhold evidence from the Commissioner.[4]

This practice of redaction or withholding of records from the Commissioner has arisen in other *HIA* reviews and received similar comment.[5] The practice is counter to the proper functioning of the review process under the *HIA*. In this case the redactions were not so extensive as to substantially impair the Commissioner's ability to complete the review. Taking a practical approach, and in the interest of providing a timely review, the Commissioner addressed the issue in the recommendations rather than insisting on full production of unredacted records. Again, the tracking tool does not address the legal obligation of providing evidence to the Commissioner as may be requested.

Recommendation #8 proposed changing the oath of confidentiality for NTHSSA employees to include references to requirements of the *Health Information Act* and to acknowledge that the

[3] This policy was promulgated pursuant to the Ministerial Directive MD-2017-03
[4] See page 87, *Health Information Act* Guide, at https://www.hss.gov.nt.ca/sites/hss/files/hia-guide.pdf
[5] See Review Report 20-HIA 32, pages 19-20

employee has received formal *HIA* training. The NTHSSA did not accept the recommendation, saying that the current oath had been developed by the Department of Health and Social Services with regard for the requirements of the *Child and Family Services Act* (*CFSA*) which NTHSSA says 'supersedes' the *Health Information Act*.[6]

Referring in the oath to both the legal obligation to protect privacy and to employee privacy training could help ensure employees are in fact aware of their duties and have taken the necessary training. In the Commissioner's view, amending the current oath is possible without creating a conflict between the actual privacy requirements of the two statutes and may help prevent this and other types of privacy breaches where lack of knowledge and training in privacy protection are root causes.

### Review Report 20-HIA 32

An individual's personal health information was used and disclosed to a third party by an NTHSSA employee without lawful authority, thereby breaching the individual's personal privacy. The incident was reported to NTHSSA by the individual on January 20, 2019, and NTHSSA confirmed a privacy breach occurred on February 27, 2019, after completing an audit of the electronic medical record. Despite the requirement under the *HIA* to notify the Commissioner in writing as soon as reasonably possible, the Commissioner only received notice on August 16, 2019, some five months later. NTHSSA provided its final report to the Commissioner on September 23, 2019.

The lack of detail in the investigation report, the delay in providing notice to the Commissioner, and other issues -- the thoroughness of the investigation, the appropriateness of the oath of confidentiality, the question of who should lead a privacy breach investigation -- led the Commissioner to conduct a review pursuant to section 137 of the *HIA*. The Review Report was issued August 12, 2020, and the NTHSSA responded by letter dated September 24, 2020.

There were 15 separate recommendations in the Review Report. NTHSSA accepted 8 of the recommendations and "deferred" 7 to the Department of Health and Social Services. These deferrals were in regard to recommended amendments to certain policy documents – the *Health Information Act Guide*, the Privacy Breach Policy created pursuant to Ministerial Directive MD-2017-03, the General Privacy and Confidentiality administrative directive AD-035 – which were being used by the NTHSSA. NTHSSA did not make a decision regarding the recommended amendments and said only that they would be forwarded to the Department for review.

The NTHSSA is a prescribed health information custodian designated under section 1(b) of the *Health Information Regulations.* A deferral of a recommendation from NTHSSA to the Department does not substantively address the recommendation: the NTHSSA said it would alert

[6] This may be a reference to section 4(1)(a) of the HIA that specifies that HIA does not apply to "a record referred to in subsection 71(1) of the *Child and Family Services Act* or any other record relating to the administration of that *Act*."

the Department of the concern, but NTHSSA did not say it would follow the recommendations or take any other course of action.

The Department was not party to this review. Strictly speaking, the Department is not the health information custodian required to respond to these recommendations. It may be reasonable for the NTHSSA to utilize policy documents developed by the Department; however, the decisions made by NTHSSA are its own decisions, and NTHSSA is responsible to ensure the policies guiding those decisions are lawful and appropriate. Where, as here, a risk of future privacy breaches is potentially associated with NTHSSA's current policies, there is a clear necessity for NTHSSA to review and, where appropriate, amend the policies it chooses to operate under.

It is a health information custodian's responsibility under section 156 of the *HIA* to decide whether to follow a recommendation made in a Commissioner's Review Report. The NTHSSA must evaluate the recommendation (and the policy at issue) and determine whether it will follow the recommendation or not. Deferring a recommendation to the Department for its review does not discharge the NTHSSA of its responsibility under section 156(1) to make a decision: it effectively amounts to a failure to decide. Under section 156(2) no decision is deemed to be a decision not to follow the recommendation.

### Review Report 20-HIA 35

This was a review of a request for access to information about which employee(s) had viewed the applicant's personal health information. The Applicant requested a Record of Activity (ROA) as contemplated by section 8 of the *Health Information Regulations*, being a "report prepared by a health information custodian in respect of an individual's personal health information." An ROA lists users who have accessed an individual's personal health information, the dates and times of access, and the information that was or could have been accessed. The Applicant believed certain sensitive personal health information (PHI) was to have been stored as a paper record, 'siloed' in a specialized health care unit. Contrary to what had been promised, the Applicant learned later that some of the PHI had been transferred into the electronic medical record (EMR) system and was then accessible by anyone with the appropriate access rights to that type of information. On May 19, 2019, the Applicant requested information about what PHI was now on the EMR, who put it there, and who had viewed it.

The Applicant was not satisfied with the ROA produced in response and sought a review by this office. The Applicant identified additional concerns about the timeliness of the response, the lack of a written response, and the sufficiency of the response. Eventually, after significant persistence of the Applicant, the NTHSSA provided additional information that, taken together with the ROA, answered most of the Applicant's questions. October 7, 2019, the Commissioner notified NTHSSA that it was undertaking a review.

The report contains seven recommendations. Four were accepted and are directed to procedural issues: the need to ensure access requests are responded to in time, in writing, and with the content specifically relevant to the request. Three of the recommendations were not accepted:

*Recommendation #4*: That NTHSSA retrieve Records of Activity (ROA) from the EMR directly to avoid unnecessary transfer, handling, and delays.

The ROA is defined in section 8 of the *HIA* regulations, and section 8(2) specifies that it is the health information custodian that shall 'process a request' by an individual under Part 5 of the *Act*. The NTHSSA exceeded the time allowed to produce the ROA under Part 5 of the *Act*.

In practice, the NTHSSA does not produce ROAs directly but instead it requests the Department to produce an ROA. This introduces potential delay and may on occasion result in the ROA not producing the information sought. Why the NTHSSA does not retrieve ROAs directly is not clear, but the fact that the Department does this for the NTHSSA does not relieve the NTHSSA of its obligation to produce the information requested within the statutory time periods.[7] Under the regulations, producing an ROA in this situation is the NTHSSA's responsibility, not the Department's. NTHSSA stated that it would provide the Department with the recommendation and "engage on discussions on this issue."

*Recommendation #5*: That NTHSSA take steps to explore and determine if the EMR can be reconfigured to capture more detailed information to better meet the requirements set out in the legislation with respect to an ROA, including minimizing inconsistencies and gaps in detail.

NTHSSA did not accept this recommendation, again indicating that the EMR was a responsibility of the Department and that it would provide the Department with the recommendation and engage on discussions on this issue. The Department appears to retain a great deal of control over the use and operation of the EMR and it seems that NTHSSA cannot independently make full use of or make changes to the EMR. However, the recommendation was "to take steps to explore and determine if the EMR system can be reconfigured." NTHSSA's statement that it will engage on discussions on this issue with the Department effectively accepts the recommendation as framed.

*Recommendation #7*: That NTHSSA review the content of the pamphlets provided to the Applicant on protection of privacy and access to information and ensure that what is written is correct and identify any discrepancies between the information in the pamphlets and the actual requirements of the legislation.

With the formal written response to the Applicant's access to information request, NTHSSA provided the Applicant with some pamphlets prepared by the Department regarding how personal information is protected, including how it is protected within the electronic health

[7] In general, under section 101(1) of the HIA, the health information custodian must respond in writing to an access request within 30 days. Under section 103, if access to the information is to be allowed and a copy is not provided with the response, the health information custodian has a further 30 days to provide a copy or otherwise provide access.

record systems. The Applicant expressed the concern that certain claims made in the pamphlets did not accord with the Applicant's experience.

Recommendation 7 was not accepted; again, NTHSSA identified the recommendation as falling under the Department's responsibility but also promised to provide the recommendation to the Department. In the review, the Commissioner noted that the pamphlets speak to an ability to provide prompt access to records such as the ROA and indicate how the electronic health systems will protect patient privacy and allow patients to exercise control over and have access to their own personal health information. The advertised claims did not match the applicant's experience and the recommendation was intended to encourage the pamphlets' content to be reviewed and amended if appropriate.

While the pamphlets are products within the Department's control, the NTHSSA is the health information custodian distributing the pamphlets. If the pamphlets contain substantive inaccuracies that is a serious issue to address. Authorship does not make their distribution of the pamphlets solely an issue for the Department. While it is clearly beneficial for the Department to be notified of the recommendation, the NTHSSA should consider for itself whether the pamphlets' information is accurate before continuing to distribute them.

# Trends and Issues

### Vaccine passports

As we emerge from the COVID-19 pandemic and public health orders are becoming less restrictive, governments in the Northwest Territories and elsewhere are exploring options for individuals to demonstrate that they have received the vaccine for COVID-19. This goes beyond providing individuals with a copy of their immunization records upon request and includes an expectation that individuals will need to demonstrate their immunization status with some certification or other guarantee of authenticity.

The idea of a vaccine passport is based on the proposition that individuals who have been vaccinated pose a lower public health risk and some restrictions can reasonably be relaxed for those people. Travelers will likely require some form of vaccination certification to facilitate travel and to reduce or eliminate the requirement to self-isolate when returning to the Northwest Territories. Such documentation will involve personal health information, which is governed by the *Health Information Act*. Vaccine passports are being proposed as a measure could facilitate travel, fewer restrictions on social gatherings, and accelerated economic recovery resulting from greater participation in society. While vaccine passports may offer substantial public benefit, they also encroach on privacy and civil liberties and should only be utilized after careful consideration.

The Federal, Provincial and Territorial Privacy Commissioners issued a joint statement on May 19, 2021,[8] identifying several potential privacy related concerns with vaccine passports. Whether for international travel or for travel within Canada, such documentation would necessarily involve the use and disclosure of personal health information governed by the *Health Information Act*. The joint statement urges governments to adhere to the 'privacy by design' principle and to work with the Privacy Commissioners to help ensure that personal information is accessed and used appropriately and is otherwise reasonably protected. The OIPC has met on this matter with officials of the Department of Health and Social Services and the Chief Information Officer and anticipates further engagement on this issue in the coming months.

## Effects of COVID 19 on Access to Information and Protection of Privacy

The pandemic has affected many aspects of government operations. Government service has experienced delays and interruptions in some areas.

In June 2020, the legislature passed an *Act*[9] allowing relief for several time related obligations, but not for the response periods specified under *Access to Information and Protection of Privacy Act* or the *Health Information Act*. Unfortunately, it has come to the attention of the Office of the Information and Privacy Commissioner that in a number of cases some public bodies had not fulfilled their duties to respond to access to information requests within the time allowed by the *ATIPPA* or *HIA*. The *ATIPPA* allows a public body 30 days to respond to a request, but also allows a public body to make a reasonable time extension. In several instances, public bodies have given notices of two or more time-extensions measured in months and still did not provide the records requested. Sometimes no notice of time extension was provided at all, amounting to a deemed refusal 30 days after the request was submitted.

Due to the incidence of lengthy delays responding to access requests, our office began to intercede informally and encourage public bodies to provide the records requested as required under the legislation. This was productive in some instances, but also served to indicate how under-resourced access to information processes are in some government departments. The delays in processing access requests also revealed problems with records management, including organization and maintenance of information and email systems. The delays have also revealed the challenge public bodies face to retain sufficient, knowledgeable, and trained staff who understand the public bodies' information and record keepings systems, including older paper systems.

While the need to maintain 'core' government services is clear, I have a sense that the access to information and protection of privacy functions are viewed by some in government as outside that 'core'. That the legislature allowed no relief from *ATIPPA* or *HIA* obligations gives a clear

[8] https://priv.gc.ca/en/opc-news/speeches/2021/s-d_20210519/

[9] *Temporary Variation Of Statutory Time Periods (Covid-19 Pandemic Measures) Act*, Bill 10. Passed June 15, 2020

signal to government that access to information and protection of privacy is in fact a core function of government.

A frequent explanation provided by public bodies for delay is that COVID-19 placed unanticipated burdens on staff to such an extent that it was not possible to meet the statutory timelines. Without doubt, the pandemic has been challenging for all and it has forced many in government to work remotely, often from home. This has presented practical challenges for providing government services. Undoubtedly, responding to access to information requests was more challenging without the normal facilities and information systems being immediately available.

Delays may also have been affected when some employees were assigned new roles or extra tasks associated with the COVID response. These and other reasons for delays in service are understandable in the context of individuals working in a system with finite staff and resources. However, the statutory obligations of a public body *as an institution* and the obligations of the head of a public body remained unchanged. Removing or reassigning resources potentially put the bureaucracy in a position of frustrating the intention of the legislature in terms of upholding the requirements of the *ATIPPA* and *HIA*. This situation caused some employees significant stress as they attempted to fulfill the statutory requirements; tasks for which they were at times under resourced and, in some cases, not properly trained. Predictably, the result was less than satisfactory, and may well have contributed to the increasing number of review requests. The Commissioner acknowledges the efforts of public bodies' staff to serve the public in these challenging circumstances and encourages public bodies to devote the necessary resources, to ensure that going forward there are sufficient staff who are properly trained and equipped to provide the access to information services set out in the legislation.

Last year's Annual Report recognized that the response to the pandemic had resulted in the collection of large amounts of personal information and personal health information in connection to the regulation of self-isolation for travelers and for people who contracted the disease or were at risk due to contact. The OIPC received notices of several significant breaches of privacy that have occurred through errors of the COVID Secretariat's use of email. In mid-March, officials with the Department of Health and Social Services advised that approximately 30 privacy breaches had occurred over the past year, many of which were associated with the COVID Secretariat. Of significant concern, no notices of these breaches had been sent to my office when the breaches were confirmed, despite the requirements of the department's Privacy Breach Policy and the *HIA*. Investigations are ongoing and the Commissioner expects to address this further in next year's Annual Report.

The COVID Secretariat was a response to an unprecedented public health emergency. Protecting the privacy interest in individuals' personal health information was an integral aspect of the response and mandated by legislation. Maintaining personal privacy requires clear communication, established privacy policy and procedures, and proper training of staff – none of which is beyond the capability of the Department of Health and Social Services or, by extension, the COVID Secretariat. Privacy policy must apply everywhere in government and should not be compromised except with the clearest of intention of the legislature as expressed in law.

The Commissioner commends those public bodies and health information custodians that report privacy breaches to my office, especially those who do so on a timely basis. It is apparent that privacy breaches are too frequently caused by staff who are under-resourced or untrained in or unaware of the policies and procedures governing privacy protection. Comprehensive and regular privacy training is often recommended by the Commissioner as a way to prevent future privacy breaches, and this type of recommendation is often accepted by public bodies. More and better training for staff is a self-evident 'good'. Yet, between the different departments and agencies subject to the *ATIPPA* and *HIA* there are wide variations in the awareness of privacy issues and the skills to respond to privacy breach events. Without doubt, providing comprehensive and regular training can be logistically challenging and expensive in terms of fiscal and human resources. However, privacy protection is not an option or 'add-on' to a public body's main purposes and responsibilities: it is fundamental. Privacy protection requires the appropriate level of resources and support from management in all departments and agencies.

Broader publication of the relevant policies and procedures may also be helpful: generally speaking, these sorts of documents should be readily accessible on the internet to government employees, the OIPC and the public alike. In responding to a recommendation in Review Report 20-HIA 26 the NTHSSA agreed to set up a website to make these policies available to staff. In Review Report 20-HIA 21, NTHSSA accepted the recommendation to publish the Health and Social Services Electronically Stored and Transferred Information Policy on its website. Making policies available to the public is a good step toward more open and transparent government.

### *ATIPPA* amendments coming into force

Amendments to the *Access to Information and Protection of Privacy Act* are expected to come into force in summer of 2021, including several significant changes:

- There are a number of clarifications of disclosure exemptions for certain types of records including records that may reveal confidences of the Executive Counsel or the Financial Management Board.
- There are sections addressing records regarding workplace investigations and employee evaluations, and records relating to business interests.
- There is a new 'public interest override' provision requiring the head of a public body to disclose information about a risk of significant harm to the environment or to health and safety of the public.
- Individuals must be given notice of breaches of personal privacy that pose a real risk of significant harm. The Commissioner must be given notice if a breach of privacy is material.
- In conducting reviews of responses to access to information requests and of breaches of privacy, the Commissioner will have jurisdiction to make orders rather than recommendations.

- Privacy Impact Assessments will have to be submitted to the Information and Privacy Commissioner for review and comment when a public body is developing a common or integrated program or service.
- As discussed below, there are a number of changes involving timelines and the review process.

The timelines set out in the *ATIPPA* to conduct reviews of access to information responses or of breaches of privacy have shortened somewhat, which entails shortened timelines for public bodies to provide documents and to make representations during the review. Often public bodies have not provided representations on a timely basis, and time extensions have been requested frequently. Now that reviews must be completed in a shorter period, such indulgences will not be available.

All parties involved will need to ensure they dedicate sufficient resources to the task of completing reviews in the time allowed by the legislation. It will not serve the public interest or the purposes of the *Acts* for the Commissioner to issue reviews without the benefit of well-prepared representations from the public bodies.

In another change to timelines, public bodies responding to access to information requests will now only be able to extend the time to respond once by their own decision. If a subsequent extension is required, a public body must first seek authorization from the Commissioner. This is a significant change: the public body will have to justify the time extension at the outset, and the Commissioner will have a new adjudicative function to discharge under the *ATIPPA*. This is not a 'rubber stamp' process: the *Act* requires the Commissioner to conduct a review of a request for a time extension and to authorize an extension only on grounds set out in section 11(1). If the past is any indication of the future, it is reasonable to expect that public bodies will be seeking time extensions frequently.

The new Access and Privacy Office (APO) in the Department of Justice has been formally acting as the coordinator for access to information requests for a number of public bodies since March of 2021. The centralization of some of the access to information functions holds real promise to improve the timeliness and quality of responses to requests by the public for access to government records. It is too early to comment other than that communication between the APO and the OIPC has been very open and cooperative. Though it risks belabouring the obvious, it bears stating that ensuring the APO maintains its cohort of trained and experienced staff will greatly assist public bodies to meet their obligations under the legislation. This should, in turn, minimize or avoid subsequent reviews by the OIPC. Getting it right the first time is undoubtedly the best approach.

Pursuant to the GNWT's Protection of Privacy Policy 82.10, Privacy Impact Assessments (PIAs) have to be submitted to the Commissioner for review and comment during the development of a proposed 'common or integrated program or service.' This will become a legal requirement when the *ATIPPA* amendments come into force. The *HIA* already requires a PIA where a health care custodian proposes a change to or a new information system or communication technology.

Best practice dictates that PIAs be prepared an early stage of a project's development in order to ensure that privacy concerns are properly addressed in the project design. Notably, the Protection of Privacy Policy specifies that a PIA must be submitted to the Commissioner for review and comment at an early stage of development, and section 42.1(4) of *ATIPPA* requires notice to the Commissioner at an early stage of developing a common or integrated program or service. Experience with some PIAs submitted under the *HIA* at a late stage in the development of a project, or even at the end, has clearly demonstrated the need to utilize PIAs early in the design process.

## Breaches of Privacy under the *Health Information Act*

Last year's Annual Report identified that most reported privacy breaches came from the Northwest Territories Health and Social Services Authority (NTHSSA). This can reasonably be attributed to the fact that NTHSSA delivers most of the health services in the Northwest Territories,[10] and to NTHSSA's improving ability to recognize privacy breaches when they occur and respond appropriately. This office has observed increased efforts by all health authorities to report privacy breach incidents, for which recognition is due.

Of the 66 privacy breach notifications received under the *HIA* last fiscal year, a concerning number related to errors in the use of fax machines to communicate personal health information. To reiterate the former Commissioner's advice, health information custodians should stop using fax machines to transmit personal health information. Responding to the Commissioner's 2018-2019 Annual Report, the Standing Committee on Government Operations' report 5-19(2) recommended that the GNWT develop and implement a plan for ending the use of fax machines in the health and social services sector. The GNWT supported this recommendation and indicated that the Department of Health and Social Services is preparing a plan to better understand the use of faxing across the health and social services system, and to continue to work toward further reducing faxing. The OIPC looks forward to an opportunity to review said plan.

Timeliness of breach reporting continues to be of concern. Section 87 of the *HIA* requires a health information custodian to provide notice of an unauthorized use or disclosure of personal health information to the affected individual and to the Commissioner as soon as reasonably possible. The Department of Health and Social Services' Privacy Breach Policy, which applies to the Department and to all health and social services authorities, requires prompt reporting as well. Nevertheless, it is a dismayingly common event that a notice of a privacy breach is received weeks or months or in some cases over a year after the health care custodian has learned of the event.

[10] NTHSSA provides health and social services for all areas except those of Hay River, which is served by the Hay River Health and Social Services Authority, and the Tłı̨chǫ communities of Behchokǫ̀, Gametic, Whatì , and Wekweètì, which are served by the Tłı̨chǫ Community Services Agency.

Sometimes the notice is provided at the same time or even in the same document as the final breach report provided to the Commissioner many months after the breach was confirmed.

Giving timely notice is essential. First, the individual whose privacy has been breached has a right to be alerted of an unauthorized use or disclosure of personal health information. Second, notice advises individuals of the right to request a review by the Information and Privacy Commissioner. Without this advice, many individuals would be unaware of the legal recourse available. Third, the Commissioner must be notified to facilitate the independent oversight function. Section 87 of the *HIA* requires notice to the affected individual and the Commissioner "as soon as reasonably possible." The existing policy and legislation framework provides the appropriate direction for health information custodians but notice of privacy breaches is, nevertheless, frequently delayed, often without justification. The OIPC will continue to monitor this issue closely going forward.

## Timely Responses to the OIPC

Timeliness is an important issue under both the *ATIPPA* and the *HIA*. If a review is requested by an individual under the *HIA*, the Commissioner must use best efforts to conclude the review within 120 calendar days.[11] When the amendments to the *ATIPPA* come into force, the time limit for completing a review will shorten from 180 calendar days to 90 business days.[12]

Following receipt of a notice of a privacy breach under the *HIA*, the OIPC will generally await receipt of a final report from the health information custodian. Depending on what is revealed and whether a request for review has been made, the Commissioner may initiate a review. This may involve seeking additional records and representations from the health information custodian. This process requires follow up, sometimes multiple times.

Notably, once the Commissioner institutes a review under the *HIA*, section 153(2) requires that the "health information custodian shall produce copies of the required records for examination by the Information and Privacy Commissioner within 14 days after receiving a request for production." [*emphasis added*] This response time is frequently not met, despite the fact that a health information custodian has no discretion to deviate from that time period and the Commissioner has no jurisdiction to extend the response time. The legislature has determined that the public interest is best served by the prompt production of records upon request by the Commissioner. Health information custodians will have to take deliberate steps to ensure they are able to act within the timeline set by the *Act*.

## Timely responses to access to information requests

The OIPC has received several complaints regarding delays in response to access to information requests under the *ATIPPA*. The *Act* currently allows a public body to extend the time to respond

[11] Section 149 of the *Health Information Act*.
[12] Section 31(3) of the *Access to Information and Protection of Privacy Act*

to a request for a reasonable period in certain circumstances. In practice, public bodies will often extend the time period more than once for the same access request. A key step in the extension procedure is notice to the applicant of the reason for the extension and advice regarding the person's right to seek a review of the extension.

In several cases there have been significant delays in a public body's response to an access to information request; in some instances, the public body eventually provided the substantive response after some communication from this office. In some of those cases this led the applicant to withdraw their request for review. In other instances, we have learned of failures to respond that have lasted for months without notice of a time extension to the applicant and without a substantive response, thus leaving the applicant with no option but to pursue a review.

While the amendments to the *ATIPPA* are not a guarantee of timely responses, a public body will now only be able to grant itself one reasonable time extension. Any further extension will be available only where authorized by the Commissioner. A willful failure to comply with the terms of such an authorization could possibly attract sanction under section 59(2)(d) of the *Act*. While the new Access and Privacy Office in the Department of Justice will no doubt be of great assistance in meeting the new timelines, not all public bodies have designated that office as their Access and Privacy Coordinator. And, notwithstanding the amendments to the *Act* and the new Access and Privacy Office, the heads of public bodies remain the persons responsible for responding to access to information requests within the time limits set by the *Act*. The heads will need to ensure their departments and agencies are ready for the changes.

## Personal Mobile Audio and Video records

The use of personal mobile devices has been a subject of scrutiny in a few reviews. Review Report 20-242 addressed the use of a personal mobile recording device to take video footage of a teacher and students in a classroom. The video file was created by an education official and later placed on a government server for general access, ostensibly for training purposes. Consent for this collection, use and disclosure had not been sought or obtained. During the Commissioner's investigation a key factor came to light: the absence of any policy direction for the use of such personal devices in the workplace. The Department of Education accepted the recommendation to develop policy in this area and indicated it would pursue this in conjunction with the GNWT Access and Privacy Office.

In another review, a counsellor left a mobile device on with an audio communication application open, resulting in a confidential conversation with a client being inadvertently shared with a third party. The potential risk for very sensitive personal information to be collected, used or disclosed without authorization is high. Given the ubiquity of personal handheld devices with video and audio recording capacity, drawing attention to associated privacy risks and providing clear policy guidance for their use by government employees is essential.

# Final Word

In our representative democracy, the public's right of access to government records is essential, subject only to the narrow exceptions set out in legislation. Similarly, the protection of individual privacy and personal information is critical to ensuring trust in government. The time and effort required to facilitate the meaningful exercise of the right of access is considerable, as is the time and effort required to design, plan, and implement protections of personal privacy. Access to information and protection of privacy requires the dedication of government resources: these tasks cannot be accomplished from 'the corner of the desk.' Trained and experienced staff, with sufficient resources and steadfast support by management, are essential to fulfilling the government's responsibilities under the *HIA* and the *ATIPPA*. Much investment and effort are required for health information custodians and public bodies to discharge their obligations.

The public's interest in accessing government records shows every sign of continuing to increase. Privacy protection issues are also likely to continue to grow as government continues to collect and use personal information. Electronic piracy, ransomware and other malware are omnipresent threats capable of wreaking considerable damage and compromising not only the ability of government to deliver services but also the security of the vast amounts of personal information held in electronic records. Diligent planning using Privacy Impact Assessments at early stages in the design of projects or programs should assist in keeping government records safe and secure.

For the foreseeable future, technology will not replace the skills and expertise of Privacy Specialists or Access to Information Coordinators working for individual departments or agencies. Dedicating resources, including a full complement of qualified, trained staff is surely the best investment to ensure the public is well served and the public bodies and health information custodians are able to discharge their duties and obligations under the legislation.

# 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@atipp-nt.ca**

**Website: www.atipp-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

20/21

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

TERRITOIRES DU NORD-OUEST

# Rapport Annuel

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

---

Kīspin ki nitawihtīn ē nīhīyawihk ōma ācimōwin, tipwāsinān.
Cree

---

Tłı̨chǫ yatı k'ǫ̀ǫ́ Dı wegodı newǫ dè, gots'o gonede.
Tłı̨chǫ

---

ʔerıhtł'ís Dëne Sųłıné yatı t'a huts'elkër xa beyáyatı theɔą ɔat'e, nuwe ts'ën yółtı.
Chipewyan

---

Edı gondı dehgáh got'ı̨e zhatıé k'ǫ́ǫ́ edatł'éh enahddhę nıde naxets'ę́ edahłí.
South Slavey

---

K'áhshó got'ı̨ne xədə k'é hederı ɔedı̨htl'é yerınıwę nídé dúle.
North Slavey

---

Jii gwandak izhii ginjìk vat'atr'ijąhch'uu zhit yinohthan jì', diits'àt ginohkhìi.
Gwich'in

---

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.
Inuvialuktun

---

ᑖᒃᑯᐊ ᑎᑎᖅᑲᐃᑦ ᐱᓕᒍᒍᐱᑦ ᐃᓄᒃᑎᑐᓪᓗᒍᒃ, ᐅᖃᖅᑎᖅᓄᑦ ᐅᖅᑰᓕᓪᓗᐊᖅ ᖃᖅᑐᑎᑦ.
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

1 juillet 2021

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

Monsieur le Président,

Conformément à l'article 68 de la *Loi sur l'accès à l'information et la protection de la vie privée* et à l'article 173 de la *Loi sur les renseignements personnels sur la santé,* j'ai l'honneur de présenter mon rapport annuel à l'Assemblée législative des Territoires du Nord-Ouest pour la période allant du 1 avril 2020 au 31 mars 2021.

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

Adresse postale : C. P. 382, Yellowknife TNO X1A 2N3
Tél. : 867-669-0976 Sans frais : 1-888-521-7088 Courriel : admin@atipp-nt.ca

# Table des matières

# Message du Commissaire

J'ai le plaisir de déposer le présent rapport annuel pour la période allant du 1er avril 2020 au 31 mars 2021, mon premier depuis ma nomination au poste de commissaire à l'information et à la protection de la vie privée le 23 novembre 2020.

Je voudrais tout d'abord saluer ma prédécesseure, Elaine Keenan Bengts, qui a occupé le poste de commissaire de façon continue depuis la création du Commissariat en 1997. Le travail inlassable de Mme Keenan Bengts pendant ces nombreuses années a permis de créer un Commissariat efficace et grandement respecté, doté d'un personnel dévoué et enthousiaste. Les rapports d'examen qu'elle a publiés ont déjà constitué et continueront de constituer une ressource précieuse pour l'application et la compréhension de notre législation.

La pandémie de COVID-19 a touché le Commissariat à l'information et à la protection de la vie privée (CIPVP) comme de nombreux employeurs. Avec quelques ajustements, le CIPVP a pu passer au travail à domicile. Dans l'ensemble, les tâches ont progressé sans subir trop de retard. C'était essentiel : il n'existait aucune dérogation légale aux délais prévus par la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*) ou la *Loi sur les renseignements personnels sur la santé* (*LRPS*), que ce soit pour les ministères ou le commissaire à l'information et à la protection de la vie privée. Plusieurs délais statutaires ont été abrégés par la loi en 2020, mais aucun ne concerne ces deux lois : une indication claire du législateur qu'il est essentiel de maintenir les activités du gouvernement ouvertes et transparentes!

Le public semble de plus en plus exercer son droit d'accès aux informations gouvernementales. Je note avec une certaine inquiétude que mon commissariat a reçu cette année un certain nombre de demandes d'examen concernant la rapidité avec laquelle certaines réponses ont été fournies à la suite de demandes d'accès à l'information. Si les organismes publics ont invoqué la pandémie comme raison des retards, l'autre problème relevé est le nombre et la portée des autres demandes d'accès à l'information auxquelles les organismes publics doivent répondre. Une plus grande utilisation des « mécanismes » d'accès à l'information laisse sous-entendre un plus grand intérêt du public à l'égard des activités du gouvernement. Bien entendu, une plus grande utilisation nécessite également un contrôle de la part du gouvernement afin que des ressources suffisantes soient en place pour permettre aux organismes publics de répondre de manière appropriée aux demandes d'accès.

L'utilisation de télécopieurs pour transmettre des renseignements personnels sur la santé continue d'être une source d'atteintes à la vie privée en vertu de la LRPS. L'utilisation du courrier électronique pour communiquer des renseignements personnels ou des renseignements personnels sur la santé a également entraîné un certain nombre d'atteintes à la vie privée. Bien que le nombre d'atteintes à la vie privée signalées au Commissariat n'ait pas diminué par rapport aux années précédentes, je suis néanmoins optimiste. En examinant les rapports sur les atteintes à la vie privée fournis en vertu de la LRPS, le Commissariat a constaté une réelle amélioration de la sensibilisation des organismes publics aux questions de protection de la vie privée et aux

pratiques exemplaires à mettre en œuvre pour le traitement approprié des renseignements personnels et des renseignements personnels sur la santé.

Il est essentiel que des politiques et des procédures efficaces de protection de la vie privée soient en place, et il est évident que les organismes publics font des efforts pour s'assurer qu'elles sont en place lorsque des lacunes ou des problèmes sont soulevés par le Commissariat. En vertu de la LRPS et de la LAIPVP respectivement, les dépositaires de renseignements sur la santé et les organismes publics devront veiller constamment à ce que les employés soient bien formés sur ces politiques et procédures et sur la bonne utilisation de la technologie. Grâce à la sensibilisation accrue à ces politiques et à ces procédures ainsi qu'à l'investissement continu dans la formation des employés sur la protection de la vie privée, on peut apporter des changements positifs dans la capacité des organismes publics à respecter et à protéger la vie privée des citoyens.

Les membres du public peuvent demander au Commissaire de vérifier si un organisme public a recueilli, utilisé ou divulgué des renseignements personnels en violation de la LAIPVP ou de la *Loi sur les renseignements personnels sur la santé*. La LRPS exige l'envoi d'un avis à la personne concernée lorsqu'une utilisation ou une divulgation non autorisée de renseignements personnels sur la santé survient. Actuellement, il n'y a pas d'exigence similaire en vertu de la LAIPVP, mais les modifications apportées à cette dernière obligeront les organismes publics à signaler les atteintes « importantes » à la vie privée au commissaire et à aviser les personnes concernées lorsqu'il est raisonnable de croire que l'atteinte crée un « risque réel de préjudice important ». En comparaison, la LRPS exige un avis au commissaire et aux personnes concernées pour toute divulgation non autorisée de renseignements personnels sur la santé. Le seuil de signalement des atteintes prévu par la LRPS peut entraîner l'envoi d'un plus grand nombre d'avis, mais il permet également de s'assurer que les personnes soient informées de la manière dont leurs renseignements personnels sur la santé sont gérés et assure une surveillance potentiellement plus efficace en soumettant les atteintes « mineures » à la vie privée à un examen minutieux afin qu'elles puissent être traitées, ce qui permet d'éviter que des événements susceptibles de causer un préjudice plus important surviennent plus tard. Bien que certains organismes publics signalent déjà les atteintes à la vie privée au Commissariat, après l'entrée en vigueur des modifications, nous nous attendons à voir une augmentation du nombre de signalements d'atteintes à la vie privée. La manière dont les organismes publics appliquent les différents seuils de signalement fera probablement l'objet d'un examen minutieux au fur et à mesure que des atteintes se produiront, et il va sans dire que nous suivrons cette question de près.

La surveillance des organismes publics et des dépositaires de renseignements sur la santé est essentielle pour garantir la protection de la vie privée et garantir au public que le gouvernement prend les mesures appropriées à cette fin. Pour protéger la vie privée des personnes, nous nous devons d'être diligents et d'assurer une gouvernance efficace avec des politiques de confidentialité et des procédures de traitement des dossiers appropriées. Il est également fondamental, pour la protection de la vie privée, de veiller à ce que les employés soient correctement formés et disposent des connaissances, des compétences et des technologies voulues. Nous sommes conscients que fournir ces garanties de confidentialité est un enjeu sérieux

où que l'on soit et peut être compliqué par la dispersion géographique et la constante mutation de la main-d'œuvre.

Pendant que le Commissariat et les organismes publics se préparent aux changements requis par les modifications de la LAIPVP, la surveillance indépendante exercée par le Commissariat aidera ces derniers à se concentrer sur les objectifs fondamentaux de la Loi : le droit du public d'accéder aux documents gouvernementaux et la protection de la vie privée. Pendant que le gouvernement, quant à lui, s'efforce de fournir des services et d'aider les citoyens des Territoires du Nord-Ouest à sortir de la pandémie, il doit également s'assurer que ces droits sont bien protégés. L'avenir s'annonce chargé, et j'ai hâte de m'attaquer au travail qui m'attend.

# Rapport financier

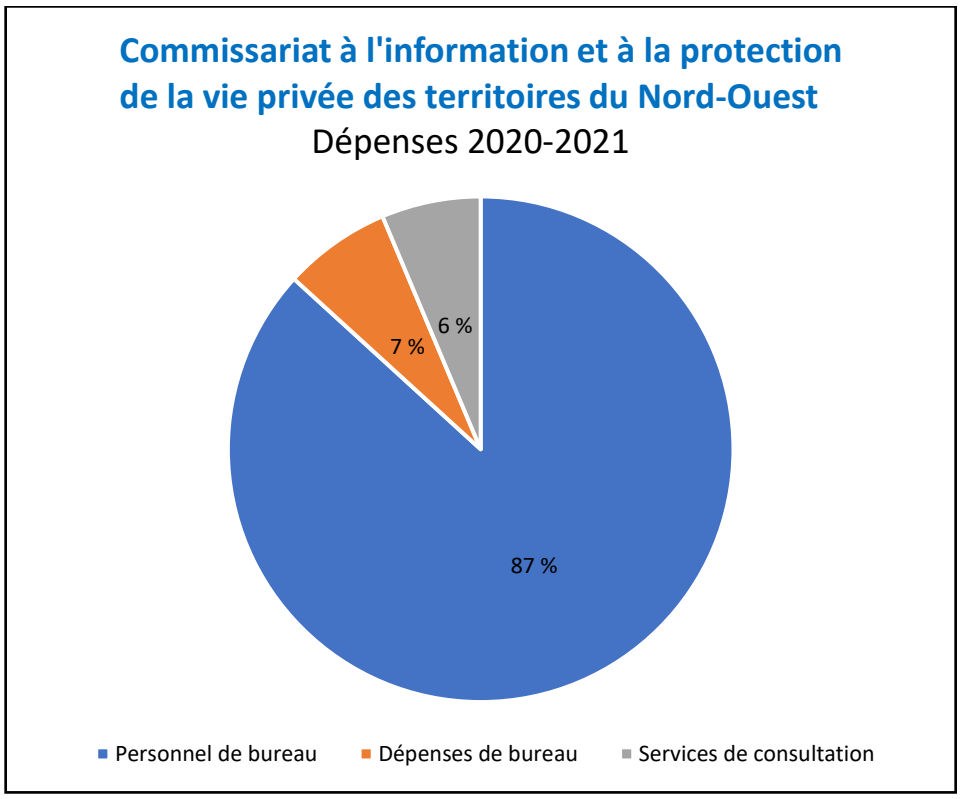
Le montant total dépensé pour assurer le fonctionnement du Commissariat à l'information et à la protection de la vie privée (CIPVP) des Territoires du Nord-Ouest pour l'exercice 2020-2021 s'est chiffré à 547 168,63 $. Les tableaux de la page suivante présentent la ventilation détaillée de ces dépenses[1].

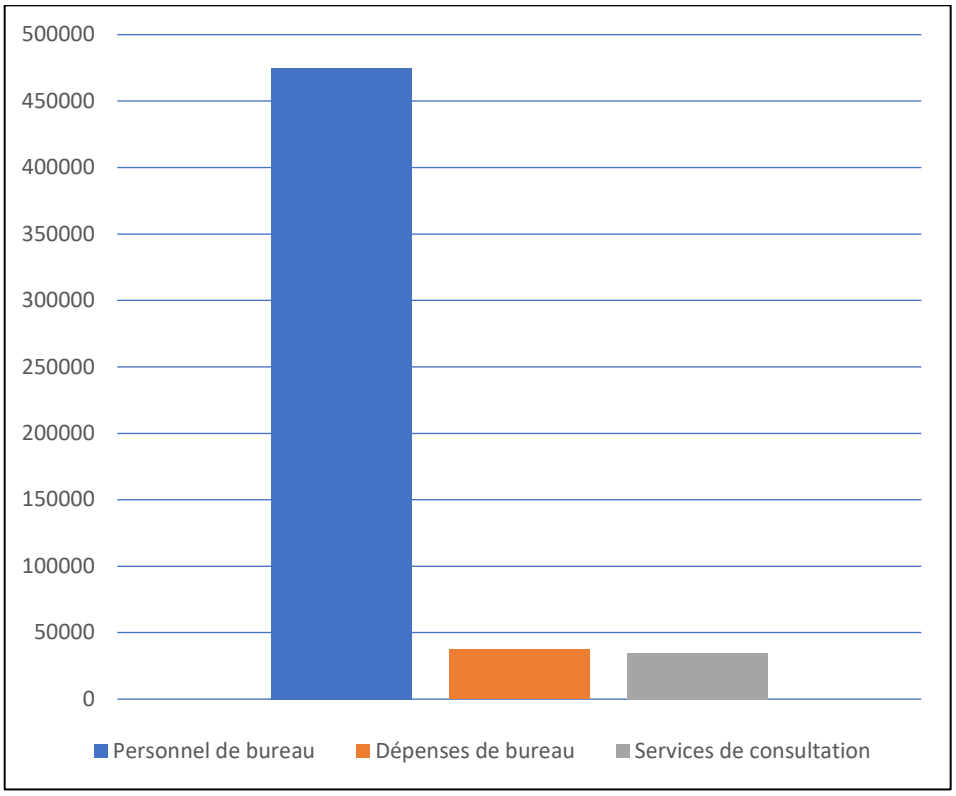
Du nouveau matériel informatique et de nouveaux logiciels ont été installés ici en décembre 2020. Immédiatement, l'utilité et la stabilité des systèmes de bureau s'en sont trouvées améliorées. Le CIPVP exprime sa reconnaissance à l'ancienne commissaire, M$^{me}$ Keenan Bengts, qui a donné la priorité à cette amélioration! Ces ajouts ont été d'une grande utilité pour tous, tant au Commissariat en tant que tel que pendant la période de travail à distance au début de l'année.

La charge de travail du CIPVP n'a cessé d'augmenter ces dernières années, et cette tendance se poursuit. À titre de comparaison, à la fin du premier trimestre de l'année dernière, le Commissariat avait ouvert 82 dossiers; pour la même période cette année, il en a ouvert 112. Pour remédier à cette situation, l'Assemblée législative a approuvé l'an dernier du financement annuel supplémentaire pour ajouter un poste d'enquêteur. Le processus d'embauche est en cours et, une fois qu'il sera terminé, la cohorte du CIPVP passera de trois à quatre.

Il reste à voir si ce niveau de dotation en personnel sera suffisant à l'avenir. Le nombre de dossiers encore à traiter est important, et l'augmentation du nombre de dossiers par rapport aux années précédentes laisse présager une demande croissante pour les services du Commissariat. Bien sûr, le mandat du CIPVP ne se limite pas à la réalisation d'examens, et les pouvoirs généraux du commissaire en vertu de l'article 67 de la LAIPVP ont été élargis dans les modifications; toutefois, notre capacité à mener des activités telles que l'éducation du public et d'autres fonctions de communication demeure assez limitée. L'examen des fonctions du CIPVP en 2019 a révélé qu'il fallait plus de personnel pour exécuter ces tâches supplémentaires. Le commissaire assurera le suivi de la situation au cours de l'année prochaine et étudiera les possibilités d'assumer pleinement toutes les responsabilités du Commissariat.

[1]En raison de la pandémie, aucune dépense de déplacement n'a été engagée cette année.


Commissariat à l'information et à la protection de la vie privée des territoires du Nord-Ouest
Dépenses 2020-2021
6 %
7 %
87 %
Personnel de bureau
Dépenses de bureau
Services de consultation


500000
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
Personnel de bureau
Dépenses de bureau
Services de consultation

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

## La *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* (LAIPVP) s'applique aux ministères, aux directions générales et aux entités du gouvernement des Territoires du Nord-Ouest ainsi qu'à 22 agences, offices, commissions, sociétés et autres organismes publics désignés dans la réglementation d'application de la Loi. La *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) consacre quatre droits et obligations clés :

- 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'exercice d'un recours indépendant à l'égard 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 Loi décrit la procédure que les membres du public doivent suivre pour obtenir accès aux documents et établit quand et comment les organismes publics peuvent collecter, utiliser ou divulguer des renseignements personnels sur des particuliers. Un examen indépendant des décisions et des actions des organismes publics est assuré par le commissaire.

## *Loi sur les renseignements personnels sur la santé*

La *Loi sur les renseignements personnels sur la santé* (LRPS) régit la collecte, l'utilisation et la divulgation des renseignements personnels sur la santé, reconnaissant à la fois le droit des personnes d'accéder à leurs renseignements personnels sur la santé et de les protéger et le besoin des dépositaires de renseignements sur la santé de recueillir, d'utiliser et de divulguer les renseignements personnels sur la santé pour soutenir, gérer et fournir des soins de santé. La Loi réglemente les dépositaires de renseignements sur la santé dans les secteurs privé et public, notamment 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 tłı̨chǫ ainsi que les médecins et les pharmaciens en pratique privée des Territoires du Nord-Ouest.

La LRPS définit les règles applicables aux fournisseurs de services de santé pour la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé et établit l'obligation pour les dépositaires de renseignements sur la santé de prendre des mesures raisonnables pour protéger la confidentialité et la sécurité des renseignements personnels sur la santé des citoyens. Elle donne également aux patients le droit de limiter la collecte, l'utilisation et la divulgation de leurs renseignements personnels sur la santé, d'imposer des conditions quant aux personnes qui ont accès à leurs dossiers de santé personnels et aux renseignements personnels sur la santé auxquelles elles peuvent avoir accès. Toutes ces dispositions sont régies par le principe selon lequel l'accès d'un fournisseur de services de santé aux renseignements personnels sur la santé d'une personne doit être limité aux informations que le fournisseur de services de santé a « besoin de connaître » pour faire son travail.

La *LRPS* exige également des dépositaires de renseignements sur la santé qu'ils avisent les personnes concernées si leurs renseignements personnels sur la santé sont utilisés ou divulgués autrement que dans les limites autorisées par la Loi ou s'ils sont volés, perdus, modifiés, ou détruits de manière inappropriée. Un avis doit être envoyé au commissaire en cas de divulgation non autorisée ou en cas d'utilisation, de perte ou de destruction non autorisée lorsqu'il existe un risque raisonnable de préjudice. Dans ces circonstances, le commissaire peut mener une enquête et produire un rapport contenant des recommandations appropriées à l'intention du dépositaire de 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 nommé sur la recommandation de l'Assemblée législative. Il relève directement de l'Assemblée législative des Territoires du Nord-Ouest et est indépendant du gouvernement.

Par l'intermédiaire du Commissariat à l'information et à la protection de la vie privée, le Commissaire s'acquitte des tâches et des fonctions énoncées dans la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et dans la *Loi sur les renseignements personnels sur la santé* (LRPS). Le CIPVP exécute un examen indépendant des décisions prises par les organismes publics et les dépositaires de renseignements sur la santé lorsqu'il répond aux demandes d'accès à l'information et enquête sur les allégations d'atteinte à la vie privée en vertu de la LAIPVP et de la LRPS. Si la réponse d'un organisme public à une demande d'accès à l'information ou à une demande de correction de renseignements personnels ne satisfait pas le requérant, celui-ci peut demander au commissaire à l'information et à la protection de la vie privée d'effectuer un examen. De même, lorsqu'une personne croit que ses renseignements personnels ou ses renseignements personnels sur la santé ont été collectés, utilisés ou divulgués sans autorisation légale, elle peut demander au commissaire à l'information et à la protection de la vie privée d'effectuer un examen. Dans certaines situations, le commissaire peut aussi procéder à un examen de sa propre initiative.

L’accès du public aux documents gouvernementaux et la protection des renseignements personnels des individus sont essentiels pour démontrer la transparence et la fiabilité du gouvernement, deux éléments indispensables à une démocratie efficace. L’accès aux documents gouvernementaux est un droit important, mais il n’est pas illimité : il existe des exceptions légales particulières — certaines obligatoires, d’autres discrétionnaires — qui permettent aux organismes publics de ne pas divulguer des dossiers. Lorsque les organismes publics décident des documents qui seront divulgués en réponse à une demande d’accès à l’information, les questions qui peuvent être soulevées sont nombreuses et peuvent être complexes. Le recours à un contrôle indépendant fait en sorte que les organismes publics respectent la législation et peut contribuer à garantir aux requérants que leurs droits sont respectés.

Le commissaire enquête sur les plaintes en obtenant d’abord l’avis des parties concernées. Dans certains cas, une résolution rapide et officieuse de l’affaire peut être possible; toutefois, il arrive fréquemment que les choses aillent plus loin. Après avoir déterminé les faits et reçu les observations du requérant, de l’organisme public et de tout tiers et après avoir appliqué les articles pertinents de la Loi, le commissaire produit un rapport qui peut contenir des recommandations à l’organisme public ou au dépositaire de renseignements sur la santé.

Les organismes publics et les dépositaires de renseignements sur la santé ne sont actuellement pas tenus d’accepter les recommandations du commissaire, mais les rapports annuels du commissaire doivent signaler les cas où un organisme public décide de ne pas suivre une recommandation. Les requérants qui ne sont pas satisfaits de la décision d’un organisme public concernant une recommandation peuvent faire appel de cette décision auprès de la Cour suprême des Territoires du Nord-Ouest.

Lorsque les modifications à la LAIPVP entreront en vigueur, le rôle du commissaire à l’information et à la protection de la vie privée changera : le pouvoir de formuler des recommandations deviendra un pouvoir de rendre des arrêtés exécutoires qui pourront être déposés à la Cour suprême des Territoires du Nord-Ouest et exécutés comme une ordonnance de la Cour. L’ordonnance d’un commissaire peut faire l’objet d’un appel devant la Cour suprême des Territoires du Nord-Ouest. Ce pouvoir de formuler des ordonnances ne s’appliquera pas aux questions relevant de la LRPS : le commissaire continuera à faire des recommandations en vertu de cette loi.

En plus de traiter les plaintes, le commissaire examine et commente les conséquences qu’ont les projets de loi ou les politiques ou programmes gouvernementaux sur la protection de la vie privée, ce qui inclut souvent l’examen et l’appréciation des évaluations des répercussions sur la vie privée. Les évaluations des répercussions sur la vie privée sont actuellement requises en vertu de la politique gouvernementale et de la LRPS et le seront dans certaines circonstances en vertu des modifications apportées à la LAIPVP.

# Bilan de l'année

Le Commissariat à l'information et à la protection de la vie privée a ouvert 162 dossiers en tout au cours de l'exercice 2020-2021. De ce total, 75 étaient des dossiers sur l'accès à l'information et la protection de la vie privée, les 87 autres étant des dossiers concernant la protection des renseignements sur la santé.

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

Entre le 1er avril 2020 et le 31 mars 2021, le CIPVP a ouvert 75 dossiers en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée.*

| | |
|---|---|
| Demandes d'examen — Accès à l'information | 26 |
| Demandes d'examen — Frais, retards et prolongation de délai | 8 |
| Demandes d'examen — Demandes de tierces parties | 4 |
| Consultations et observations — Lois, législations, projets de loi | 8 |
| Questions relatives à la vie privée — Atteintes et plaintes | 26 |
| Corrections – aux renseignements personnels | 1 |
| Divers et administratif | 2 |

## *Loi sur les renseignements personnels sur la santé*

Entre le 1er avril 2020 et le 31 mars 2021, le CIPVP a ouvert 87 dossiers en vertu de la *Loi sur les renseignements personnels sur la santé.*

| | |
|---|---|
| Signalements pour atteinte à la vie privée | 66 |
| Demande d'examen — Atteinte à la vie privée | 10 |
| Observations — Évaluations des répercussions sur la vie privée | 7 |
| Observations — Politiques, lois et processus en matière de santé | 3 |
| Divers et administration | 1 |

## Rapports d'examen — *Loi sur l'accès à l'information et la protection de la vie privée*

En 2020-2021, 28 rapports d'examen ont été publiés en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*. Ces rapports traitent des examens des réponses aux demandes d'accès à l'information en vertu de l'article 28 de la *LAIPVP* et des examens de la collecte, de l'utilisation ou de la divulgation non autorisée de renseignements personnels en vertu de l'article 49.1. Les examens effectués en vertu de l'article 28 portent sur le caractère suffisant et opportun des réponses aux demandes d'accès à l'information et sur les répercussions possibles sur la vie privée des tiers dont les renseignements personnels étaient visés par la demande d'accès à l'information. Les examens relatifs à l'article 49.1 ont pour but de déterminer si les renseignements personnels ont été collectés, utilisés ou divulgués sans autorisation légale. Les rapports sont disponibles en ligne sur https://www.canlii.org/fr/nt/ntipc/[2].

L'article 68 de la *Loi sur l'accès à l'information et la protection de la vie privée* exige que le rapport annuel contienne des renseignements sur les cas où les recommandations du commissaire à l'information et à la protection de la vie privée formulées dans le cadre d'un examen n'ont pas été suivies. Il s'agit notamment de cas où l'organisme public a négligé de répondre aux recommandations du commissaire dans les 30 jours suivant la réception d'un rapport d'examen, ce qui constitue un refus présumé d'accepter les recommandations. Dans la plupart des cas, les organismes publics n'avaient pas l'intention de rejeter les recommandations et n'étaient pas au fait des dispositions de présomption. La plupart de ces cas ont été résolus par une correspondance de suivi, bien que certains aient nécessité un suivi répété avant l'émission d'un avis de décision.

Voici les résumés des rapports d'examen pour lesquels l'organisme public a décidé de ne pas suivre les recommandations du commissaire.

### Rapport d'examen 20-226

Il s'agissait de l'examen d'une réponse à une demande d'accès à l'information déposée en 2019 auprès de la Division des ressources humaines du ministère des Finances. La réponse contenait des courriels entre fonctionnaires discutant d'aspects de la situation professionnelle du candidat. L'organisme public a effectué de nombreux caviardages dans les dossiers en vertu du paragraphe 14 (1) de la *Loi sur l'accès à l'information et la protection de la vie privée*, qui permet à l'organisme public de refuser de divulguer un dossier dont on pourrait raisonnablement s'attendre à ce qu'il révèle certains types de renseignements, tels que a) des avis, des propositions, des recommandations, des analyses ou des options stratégiques élaborées pour un organisme public ou b) des consultations ou des délibérations auxquelles ont participé des dirigeants ou des

[2]Les décisions des années précédentes sont également disponibles en ligne dans cette base de données publique gratuite.

employés d'un organisme public. Le requérant a demandé un examen du caviardage effectué dans divers documents.

Le commissaire à l'information et à la protection de la vie privée a recommandé que plusieurs parties des documents qui avaient été caviardées soient divulguées. Le Ministère a accepté tout, sauf deux paragraphes d'un courriel. Le Ministère continue de considérer que les deux paragraphes contiennent des avis et qu'ils ne devraient pas être divulgués. Le rapport du commissaire contient une explication informative du paragraphe 14(1) et des types de renseignements que ce paragraphe vise. Le Ministère n'a pas fourni d'autres informations ou explications sur sa décision de maintenir le caviardage. Le demandeur s'est retrouvé avec une simple affirmation indiquant que les paragraphes contenaient des « avis du Ministère ».

## Rapport d'examen 20-228

Le 27 mai 2019, le requérant a fait une demande d'accès à l'information auprès du ministère de la Santé et des Services sociaux. Le Ministère a recensé 21 pages de documents divulgables, mais a refusé l'accès à tous les documents en évoquant le paragraphe 23(1) de la *Loi sur l'accès à l'information et la protection de la vie privée* et en déclarant que la divulgation de l'information entraînerait une atteinte déraisonnable à la vie privée d'un individu. En refusant l'accès, le Ministère a indiqué que les renseignements demandés étaient des renseignements sur l'emploi, les antécédents professionnels et éducatifs d'un tiers et des renseignements personnels relatifs à l'embauche et à la gestion d'un tiers.

Au début de l'examen, et à la suggestion du commissaire, le Ministère a divulgué les 21 pages de documents au requérant, mais en les caviardant considérablement. Le Ministère a évoqué les alinéas 14(1)a) et 23(2)d) de la Loi pour justifier le caviardage. L'examen des documents divulgués sous forme caviardée s'est poursuivi.

Au cours de l'examen, le Ministère a formulé des observations écrites afin d'expliquer son application de la Loi. Le commissaire a estimé que les raisons invoquées par le Ministère ne répondaient pas aux exigences de la Loi et a recommandé que l'accès aux documents soit accordé avec beaucoup moins de caviardage. Le Ministère a décidé de ne pas suivre certaines des recommandations en retenant certains documents et en citant un article de la Loi qui n'a pas été invoqué lors de l'examen.

Il s'agit d'une situation très problématique : la Loi ne prévoit pas de processus par lequel un organisme public peut tester l'application de différents articles de manière itérative. Au cours d'un examen, un organisme public a la possibilité de formuler des observations écrites complètes afin que les raisons de la décision initiale de refuser l'accès à un document puissent être dûment examinées par le commissaire. Le rejet de la recommandation d'un commissaire pour des raisons qui ne sont pas exposées dans les observations de l'organisme public prive effectivement le commissaire du raisonnement de l'organisme public. Cela peut empêcher le requérant d'avoir la possibilité de faire examiner toutes les questions pertinentes par le commissaire. Il s'agit d'un aspect important de l'équité procédurale. Une telle approche laisse entrevoir un manque de diligence à fournir au commissaire des représentations complètes en première instance et peut

également suggérer que l'intention de ne pas divulguer certaines parties d'un document découle d'un intérêt autre qu'une application bien réfléchie de la Loi. Un organisme public doit fournir tous les éléments de preuve et tous les arguments sur lesquels il a l'intention de s'appuyer lorsqu'il formule des observations à l'intention du commissaire au cours d'un examen.

## Rapport d'examen 20-229

Le présent rapport examine la réponse du ministère de l'Industrie, du Tourisme et de l'Investissement à une demande d'accès à l'information portant sur des courriels et des pièces jointes concernant le requérant et son entreprise. Le Ministère a dressé une liste de 4 602 documents pouvant être divulgués pour la période visée, dont beaucoup étaient des courriels en double. La plupart des documents ont été divulgués dans leur intégralité ou avec un minimum de caviardage. Le Ministère a procédé au caviardage de quelques passages en vertu de l'article 23, qui régit la protection des renseignements personnels de tiers, et en vertu des alinéas 14(1)a) et b), qui permettent à un organisme public de refuser de divulguer des renseignements dont on peut raisonnablement s'attendre à ce qu'ils révèlent des avis, des propositions, des options politiques, etc., élaborés pour un organisme public ou un membre du Conseil exécutif ou dont la divulgation révélerait des consultations ou des délibérations auxquelles ont participé des dirigeants ou des employés d'un organisme public. Le requérant a demandé un examen des passages caviardés.

Le commissaire a recommandé que plusieurs passages caviardés le demeurent, mais dans certains cas pour des raisons différentes de celles fournies par l'organisme public. Dans certains cas, le commissaire a recommandé une réduction du caviardage par rapport à celui proposé par l'organisme public. Dans d'autres cas, le commissaire a recommandé au Ministère de reconsidérer le caviardage de certains renseignements à la lumière de l'application possible de l'article 24 de la Loi, qui protège certains types de renseignements « d'intérêt commercial ». Dans d'autres cas encore, le commissaire a recommandé au Ministère de reconsidérer le caviardage en vertu des alinéas 14(1)a) ou b), lesquels exigent l'application d'un pouvoir discrétionnaire par l'organisme public.

Sur les 39 recommandations distinctes visant à divulguer davantage de renseignements, 36 ont été acceptées en totalité, et trois en partie. Le Ministère a fourni des explications sur le maintien de certains passages caviardés en évoquant des préoccupations particulières concernant la sensibilité potentielle de certaines informations. Dans chaque cas, les passages caviardés ne différaient des recommandations du commissaire qu'à l'égard de quelques mots. Le commissaire a formulé dix autres recommandations visant à revoir l'application des articles 23 ou 24 ou l'exercice du pouvoir discrétionnaire en vertu du paragraphe 14(1) et, dans tous les cas, l'organisme public a divulgué des renseignements supplémentaires et a exposé ses motifs.

### Rapport d'examen 20-230

Le ministère des Infrastructures a répondu à une demande d'accès à l'information portant sur des courriels et des pièces jointes concernant le requérant et son entreprise. Le commissaire a remis le rapport d'examen au Ministère le 21 mai 2020. Le Ministère a répondu au requérant par une lettre datée du 2 juillet 2020, mais n'a pas informé le commissaire avant le 2 octobre 2020, après l'envoi de lettres d'enquête par le CIPVP le 17 juillet 2020, puis le 1er octobre 2020. En vertu de l'article 36 de la Loi, un organisme public dispose de 30 jours pour informer le commissaire de sa décision concernant toute recommandation.

Les documents produits pour le requérant ont été examinés sous la forme de quatre « ensembles » distincts totalisant 902 pages. Le deuxième dossier contenait 171 pages, dont trois — un tableau des demandes d'indemnisation pour accidents du travail — ont été largement caviardées en raison de leur « pertinence ». Or, la pertinence n'est pas un motif de non-divulgation en vertu de la Loi. Le commissaire a recommandé que ces trois pages de caviardage soient réexaminées par le Ministère afin de déterminer si l'une des exceptions prévues aux articles 13 à 25 de la Loi s'appliquait à l'un des documents. Le commissaire a proposé que « le nom de l'organisation, la date de l'accident, la date d'enregistrement à la CSTIT, la catégorie de demande, la pénalité de retard et le lieu soient autant de renseignements qui pourraient être divulgués sans entraîner une atteinte déraisonnable à la vie privée ». Le Ministère a décidé de divulguer la plupart des informations contenues dans ces trois pages, à l'exception de la localisation des personnes, afin de s'assurer qu'aucun tiers ne puisse être identifié. Cette recommandation s'applique également à trois tableaux similaires dans le deuxième ensemble de documents. Pratiquement toutes les recommandations du commissaire ont été acceptées, sauf le lieu où vivent les requérants.

## Rapports d'examen — *Loi sur les renseignements personnels sur la santé*

Douze rapports d'examen ont par ailleurs été publiés en vertu de la *Loi sur les renseignements personnels 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/. Les rapports passent en revue divers cas de collecte, d'utilisation ou de divulgation non autorisées de renseignements personnels sur la santé.

Dans certains cas, les renseignements personnels d'une personne ont été incorrectement identifiés dans les dossiers papier ou électroniques ou divulgués aux mauvaises personnes. Il n'est pas rare que des renseignements personnels sur la santé soient illégalement divulgués lors de l'utilisation de télécopieurs pour transmettre des renseignements personnels sur la santé. Ce point a fait l'objet de commentaires de la part de la commissaire dans les rapports annuels des années précédentes, et plus récemment dans les rapports 20-LRPS 26 et 20-LRPS 27 de cette année. Bien que les dépositaires de renseignements sur la santé se soient engagés à réduire l'utilisation des

télécopieurs dans la prestation des services de santé, les erreurs liées à l'utilisation des télécopieurs continuent de générer des rapports sur des télécopieurs mal gérés, des télécopies mal acheminées, des lacunes dans la formation et d'autres problèmes entraînant la divulgation illégale de renseignements personnels sur la santé.

Les renseignements personnels sur la santé sont intrinsèquement sensibles, et les atteintes à la vie privée concernant ces informations sont toujours préoccupantes. Un événement particulièrement significatif s'est produit en juillet 2019 : des dossiers de patients de l'ancien hôpital territorial Stanton ont été trouvés par un particulier à la décharge de déchets solides de Yellowknife. Des disques compacts avec l'identification des patients ont été trouvés à côté d'autres déchets provenant de l'hôpital désaffecté. Après avoir mené une enquête préliminaire, l'ASTNO a engagé des enquêteurs indépendants pour mener une enquête officielle. Malheureusement, les enquêteurs n'ont pu exécuter leur travail, car le personnel de l'installation de traitement des déchets avait réuni les déchets, les avait mis en ballots et les avait enterrés avant que les enquêteurs ne se rendent sur les lieux. Bien que cela ait probablement limité toute autre atteinte potentielle à la vie privée, il a également été difficile d'identifier les personnes concernées et de déterminer les détails des renseignements personnels sur la santé en cause. Le commissaire a reçu le rapport d'enquête de l'ASTNO et le dossier de preuves, bien que certaines parties de certaines pages manquent dans le rapport et qu'il y ait un petit nombre de passages caviardés. Le rapport 20-LRPS 31 du commissaire a abordé une série de questions concernant les circonstances qui ont conduit à l'infraction et la réponse à cette atteinte. Les enjeux portaient sur divers aspects de l'entreposage et du transfert des dossiers, l'utilisation et la formation des entrepreneurs lors de la manipulation des renseignements personnels sur la santé, les méthodes visant à limiter les risques et à atténuer toute divulgation illégale de renseignements personnels sur la santé, la planification et la coordination de projets multiservices, la destruction des preuves, le manque de rapidité dans le signalement des infractions à l'ASTNO, le manque de coordination des activités et des acteurs lors du déménagement de l'hôpital, etc. Le commissaire a proposé 27 recommandations distinctes. L'ASTNO a tout accepté, comme elle l'a indiqué dans sa lettre du 29 mai 2020.

Le paragraphe 173(b) de la *Loi sur les renseignements personnels sur la santé* exige que le rapport annuel du commissaire traite des recommandations formulées dans le cadre d'un examen et qui n'ont pas été suivies par le dépositaire de renseignements sur la santé. Voici des résumés des rapports d'examen dans lesquels le dépositaire de renseignements sur la santé a décidé de ne pas suivre les recommandations du commissaire.

### Rapport d'examen 20 — LRPS 24

Cet examen portait sur un cas où un médecin suppléant — un médecin engagé à titre temporaire, souvent d'une autre province ou d'un autre territoire — a accédé au dossier médical d'un patient sans autorisation et à une fin non liée aux soins dispensés à ce patient ou autrement autorisée par la Loi. Le médecin a accédé au dossier du patient B dans le système de dossiers médicaux électroniques (DME) lors d'un rendez-vous avec le patient A, prétendument dans le but d'évaluer la situation médicale de cette dernière. Le médecin a noté certains détails des renseignements personnels sur la santé du patient B dans le dossier DME du patient A. Le patient B n'était pas au courant et n'a pas consenti à l'accès ou à la divulgation de ces renseignements personnels sur la santé. Il n'y avait aucune justification légale pour le médecin d'accéder aux dossiers du patient B. Le médecin a affirmé que ce type d'accès aux dossiers médicaux d'un tiers était une pratique courante dans son lieu de pratique d'origine, mais le Collège des médecins et chirurgiens de cette province a confirmé le contraire.

D'autres problèmes ont aussi été relevés au cours de l'enquête du commissaire. Tout d'abord, l'atteinte s'est produite en juin 2018, mais n'a été signalée au commissaire ou au patient B qu'en avril 2019 — soit neuf mois plus tard — même si l'infraction a été découverte par un autre praticien de la santé peu après l'incident. Deuxièmement, les informations contenues dans les avis d'atteinte adressés à la personne concernée et au CIPVP n'étaient pas suffisamment détaillées pour que l'on puisse comprendre la nature de l'infraction. Troisièmement, le dépositaire des renseignements sur la santé — l'Administration des services de santé et des services sociaux des Territoires du Nord-Ouest (ASTNO) — a résisté à l'idée de retirer la référence aux renseignements du patient B des dossiers médicaux du patient A, malgré le fait qu'il s'agissait d'un cas d'utilisation illégale des renseignements personnels sur la santé du patient B.

Le commissaire à l'information et à la protection de la vie privée a formulé sept recommandations pour remédier à la situation. Elles portaient sur les points suivants :

(a) Mesures disciplinaires possibles pour le médecin, conformément aux règlements de l'ASTNO, aux règlements de la *Loi sur les renseignements personnels sur la santé* et à l'article 185 de la *Loi sur les renseignements personnels sur la santé*, qui considère comme une infraction le fait de collecter, d'utiliser ou de divulguer sciemment des renseignements personnels sur la santé en violation de la Loi;
(b) Nécessité de s'assurer et de documenter que tout le personnel, y compris les médecins suppléants, suit une formation appropriée sur la protection de la vie privée avant de fournir des services de santé et de traiter des renseignements personnels sur la santé;
(c) Retrait des mentions concernant les renseignements personnels sur la santé du patient B des dossiers du patient A et inscription dans les dossiers du patient B d'une mention indiquant que cette divulgation a eu lieu;
(d) Nécessité de signaler rapidement les violations aux individus et au CIPVP, de manière détaillée et précise.

L'ASTNO n'a pas accepté les recommandations concernant la discipline des médecins ou la modification des dossiers médicaux des patients. La dernière était expressément soumise à « l'attente d'un avis juridique », ce qui laisse sous-entendre que la question allait être examinée plus en profondeur. L'ASTNO a précisé sa décision concernant une éventuelle mesure disciplinaire, en disant qu'elle « suivrait le processus en place décrit dans la réglementation applicable des TNO pour s'assurer que toute préoccupation concernant un médecin fait l'objet d'une enquête et que les mesures nécessaires soient prises ».

### Rapport d'examen 20 — LRPS 28

En août 2019, le ministère de la Santé et des Services sociaux a informé le CIPVP qu'un employé du Ministère avait envoyé par erreur à un proche d'un patient une copie de certains renseignements personnels sur la santé (RPS) liés à la demande de déplacement du patient POUR raisons médicales. Les RPS ont été envoyés intentionnellement; l'employé ne s'est pas rendu compte à ce moment-là que ce n'était pas approprié. L'employé occupait temporairement un poste sans connaissances ni formation appropriées. Avant d'envoyer l'information, l'employé avait consulté le bon manuel de programme et demandé conseil à un collègue. Ni l'employé ni le collègue n'ont demandé conseil au responsable de l'unité. Les RPS qui ont été divulgués comprenaient des informations sur les coordonnées personnelles, le numéro de soins de santé personnel et le but médical du déplacement.

Bien que l'erreur ait été détectée presque immédiatement, et par plus d'un membre du personnel, le signalement initial de l'infraction a été retardé, car personne à l'époque n'a reconnu que la divulgation au parent du patient n'était pas autorisée en vertu de la *Loi sur les renseignements personnels sur la santé*. Dans son rapport d'examen, le commissaire a évalué les causes potentielles de l'infraction, les mesures de protection de la vie privée en place et la réponse du Ministère à l'infraction. Il a traité de la nécessité d'une formation sur la protection de la vie privée et sur la réponse aux atteintes à la vie privée et a formulé des observations sur le risque de divulgation non autorisée de renseignements personnels sur la santé inhérent aux formulaires de déplacements médicaux utilisés.

La commissaire a formulé huit recommandations à l'intention du Ministère pour traiter les différents aspects de cette atteinte à la vie privée en vue de prévenir d'autres situations du genre à l'avenir. Le rapport d'examen a été soumis au ministre avec une lettre datée du 11 mai 2020. Des lettres de suivi visant à obtenir une réponse du ministre ont été envoyées le 24 juin 2020 et le 12 août 2020. En septembre, le Ministère a envoyé un courriel reconnaissant le retard et indiquant qu'une réponse était attendue dans deux ou trois semaines. Le commissaire à l'information et à la protection de la vie privée a envoyé d'autres rappels de suivi le 1er octobre 2020, et enfin le 12 novembre 2020.

Si le dépositaire de renseignements sur la santé omet de communiquer un avis de décision concernant les recommandations du commissaire dans les 30 jours suivant la réception d'un rapport d'examen, le paragraphe 156(2) de la *Loi sur les renseignements personnels sur la santé*

considère alors qu'il s'agit d'une décision de ne pas suivre les recommandations. Le 30 juin 2021, soit un an après que la décision du ministre ait été requise, mon bureau a reçu un avis de décision du Ministère acceptant les huit recommandations. Ce retard a été attribué en grande partie à des priorités concurrentes liées à la réponse à la pandémie. Comme nous l'avons mentionné plus haut, le législateur n'a accordé aucune dérogation aux délais prévus par la LRPS, malgré les problèmes posés par la pandémie.

### Rapport d'examen 20 — LRPS 30

Le 21 mars 2019, un employé de l'ASTNO a découvert des papiers contenant des renseignements personnels et des renseignements personnels sur la santé de 109 personnes dans une maison des membres du personnel d'une petite communauté. La maison avait été occupée à différents moments par divers membres du personnel de l'ASTNO en 2017 et 2018. Les papiers avaient été abandonnés et laissés sans surveillance. Chaque employé avait laissé des documents là. La maison, qui avait été cambriolée en décembre 2018, pourrait avoir été occupée pendant une courte période par des inconnus. On ne sait pas si des tiers ont lu ou éliminé certains de ces documents. L'enquête de l'ASTNO a relevé, entre autres, un manque de connaissances et de formation des employés locaux sur la protection de la vie privée et la gestion des dossiers.

Après avoir reçu l'avis de l'ASTNO concernant l'atteinte à la vie privée, le commissaire a procédé à un examen de l'incident conformément à l'article 137 de la LRPS. Le commissaire a soulevé quelques autres préoccupations, notamment un avis tardif et inadéquat aux personnes dont la vie privée a été violée et un retard déraisonnable dans la remise du rapport d'enquête final de l'ASTNO au commissaire. Le commissaire a également noté que plus de détails dans la description des documents auraient été utiles pour déterminer la sensibilité des informations et les mesures à mettre en œuvre pour protéger ces informations.

Au cours de l'examen, il est apparu que l'enquête de l'ASTNO n'était pas principalement axée sur l'atteinte à la vie privée. Il ne fait aucun doute que l'ASTNO était préoccupée par d'autres considérations, mais celles-ci n'auraient pas dû nuire à l'objectif de mener une enquête complète et détaillée sur l'atteinte à la vie privée, comme le prévoit la Politique sur les atteintes à la vie privée (2017). Les autres exigences légales ou politiques ne supplantent pas ou ne remplacent pas l'exigence d'une enquête approfondie sur la protection de la vie privée, qui est essentielle pour que nous puissions comprendre la gravité de l'infraction et nous assurer que des mesures appropriées sont prises pour éviter qu'elle ne se reproduise.

Le commissaire a formulé huit recommandations dans son rapport du 21 juillet 2020; trois n'ont pas été acceptées.

La recommandation n$^{o}$ 5 suggérait que l'ASTNO élabore un plan d'enquête pour les cas impliquant des infractions potentielles concernant des renseignements personnels sur la santé et d'autres renseignements personnels. L'ASTNO n'a pas accepté cette recommandation dans un premier temps, mais a déclaré qu'elle devait être revue après avoir obtenu des précisions supplémentaires.

Dans une lettre de suivi datée du 5 novembre 2020, l'ASTNO a déclaré qu'elle partagerait la recommandation avec le comité de gestion des risques pour la qualité de l'organisation, qui implique à la fois l'ASTNO et le ministère de la Santé et des Services sociaux. Dans une lettre datée du 27 avril 2021, l'ASTNO a indiqué qu'elle avait rédigé une politique sur les atteintes à la vie privée pour traiter les atteintes à la fois à la *Loi sur les renseignements personnels sur la santé* et à la *Loi sur l'accès à l'information et la protection de la vie privée*. La manière dont cette politique s'aligne sur la politique du ministère de la Santé et des Services sociaux en matière d'atteinte à la vie privée n'est pas tout à fait claire[3],mais il semble que l'ASTNO ait maintenant accepté cette recommandation, du moins en partie.

La recommandation n$^{o}$ 6 proposait que l'ASTNO s'assure de fournir au commissaire, sur demande, toutes les informations que ce dernier peut exiger aux fins de toute enquête sur le non-respect de la LRPS. L'ASTNO a initialement décidé de ne pas accepter cette recommandation, mais de la transmettre au ministère de la Justice pour qu'il donne son avis. Plus tard, dans sa lettre du 5 novembre 2020, l'ASTNO a fait référence à l'élaboration d'une politique sur l'atteinte à la vie privée. Dans sa lettre du 27 avril 2021, ses responsables ont indiqué qu'elle avait mis en place un nouvel outil de suivi qui permettra de s'assurer que les signalements et les réponses au commissaire sont effectués rapidement.

Cet outil de suivi sera sans aucun doute utile, mais la recommandation portait non pas sur la rapidité des réponses, mais sur leur exhaustivité. Au cours de l'examen du commissaire, l'ASTNO s'est opposée à la production d'une copie non caviardée de son rapport d'enquête final au commissaire. C'était inapproprié : l'article 154 de la Loi donne au commissaire le pouvoir d'exiger la production de documents; de plus, le guide de la *Loi sur les renseignements personnels sur la santé* produit par le ministère l'exige :

> Les dépositaires doivent produire tous les documents dont le commissaire a besoin. Ceux-ci doivent être produits dans les 14 jours. Le commissaire peut consulter les dossiers (par exemple, sur les systèmes électroniques d'information sur la santé) si des copies ne peuvent être produites dans les 14 jours. Le commissaire peut exiger la présentation de toute preuve et n'est pas tenu de s'en tenir aux règles du tribunal. Personne ne peut dissimuler des preuves au commissaire[4].

Cette pratique de caviardage ou de rétention de documents demandés par le commissaire a été observée dans d'autres examens en vertu de la LRPS et a fait l'objet de commentaires similaires[5]. Cette pratique va à l'encontre du bon fonctionnement du processus d'examen de la LRPS. Les caviardages n'étaient pas si importants au point de diminuer de manière substantielle la capacité du commissaire à mener à bien l'examen. Adoptant une approche pratique, et dans l'intérêt de fournir un examen en temps opportun, le commissaire a abordé la question dans les recommandations plutôt que d'insister sur la production complète de documents non censurés.

[3]La politique a été promulguée en vertu de la directive ministérielle MD-2017-03.
[4]Voir page 87, Guide de la *Loi sur les renseignements personnels sur la santé*, à https://www.hss.gov.nt.ca/sites/hss/files/hia-guide.pdf.
[5]Voir Rapport d'examen 20-HIA 32, pages 19-20.

Là encore, l'outil de suivi ne répond pas à l'obligation légale de fournir des preuves au commissaire.

La recommandation nº 8 proposait de modifier le serment de confidentialité des employés de l'ASTNO afin d'y inclure des références aux exigences de la *Loi sur les renseignements personnels sur la santé* et d'y confirmer que l'employé a reçu une formation officielle sur la LRPS. L'ASTNO n'a pas accepté cette recommandation, affirmant que le serment actuel avait été élaboré par le ministère de la Santé et des Services sociaux en tenant compte des exigences de la *Loi sur les services à l'enfance et à la famille* (LSEF) qui, selon l'ASTNO, a préséance sur la *Loi sur les renseignements personnels sur la santé*[6].

Le fait d'évoquer dans le serment à la fois l'obligation légale de protéger la vie privée et de confirmer la formation des employés sur la protection de la vie privée pourrait garantir que les employés sont effectivement conscients de leurs devoirs et ont suivi la formation nécessaire. Selon le commissaire, il est possible de modifier le serment actuel sans créer de conflit entre les exigences réelles des deux lois sur la protection de la vie privée, et cela pourrait contribuer à prévenir ce type d'atteinte à la vie privée et d'autres types d'atteintes à la vie privée dont la cause première est le manque de connaissances et de formation dans le domaine.

### Rapport d'examen 20 — LRPS 32

Les renseignements personnels sur la santé d'une personne ont été utilisés et divulgués à un tiers par un employé de l'ASTNO sans autorisation légale, portant ainsi atteinte à la vie privée de ladite personne. L'incident a été signalé à l'ASTNO par la personne le 20 janvier 2019, et l'ASTNO a confirmé qu'une atteinte à la vie privée s'était produite le 27 février 2019 après avoir effectué un audit du dossier médical électronique. Malgré l'obligation, en vertu de la LRPS, d'informer le commissaire par écrit dès que cela est raisonnablement possible, la commissaire n'a reçu l'avis que le 16 août 2019, soit quelque cinq mois plus tard. L'ASTNO a remis son rapport final à la commissaire le 23 septembre 2019.

Le manque de détails dans le rapport d'enquête, le retard dans la transmission de l'avis à la commissaire et d'autres problématiques — la rigueur de l'enquête, la pertinence du serment de confidentialité, la question de savoir qui devrait diriger une enquête sur une atteinte à la vie privée — ont amené la commissaire à effectuer un examen en vertu de l'article 137 de la LRPS. Le rapport d'examen a été publié le 12 août 2020, et l'ASTNO a répondu par une lettre datée du 24 septembre 2020.

Le rapport d'examen contenait 15 recommandations distinctes. L'ASTNO a accepté 8 des recommandations et en a « transféré » 7 au ministère de la Santé et des Services sociaux. Ces reports concernaient les modifications recommandées pour certains documents de politique — le

[6] Il peut s'agir d'un renvoi à l'alinéa 4(1)a) de la LRPS qui précise que la LRPS ne s'applique pas aux documents visés au paragraphe 71(1) de la *Loi sur les services à l'enfance et à la famille* ou à tout autre document relatif à l'application de cette loi.

Guide de la *Loi sur les renseignements personnels sur la santé*, la Politique sur les atteintes à la vie privée créée en vertu de la directive ministérielle MD-2017-03, la Directive administrative générale sur la protection de la vie privée et la confidentialité AD-035 — qui étaient utilisés par l'ASTNO. L'ASTNO n'a pas pris de décision concernant les modifications recommandées et a seulement déclaré qu'elles seraient transmises au Ministère pour examen.

L'ASTNO est un dépositaire de renseignements sur la santé désigné en vertu du paragraphe 1(b) du *Règlement sur les renseignements sur la santé.* Le renvoi d'une recommandation de l'ASTNO au Ministère ne répond pas de manière substantielle à la recommandation : l'ASTNO a dit qu'elle alerterait le Ministère de la situation, mais l'ASTNO n'a pas dit qu'elle suivrait les recommandations ou qu'elle prendrait une quelconque autre mesure.

Le Ministère n'a pas participé à cet examen. À proprement parler, le Ministère n'est pas le dépositaire de renseignements sur la santé tenu de répondre à ces recommandations. Il peut être raisonnable pour l'ASTNO d'utiliser les documents de politique élaborés par le Ministère; cependant, les décisions prises par l'ASTNO sont ses propres décisions, et l'ASTNO doit s'assurer que les politiques guidant ces décisions sont légales et appropriées. Lorsque, comme dans le cas présent, un risque d'atteinte future à la vie privée est potentiellement associé aux politiques de l'ASTNO, il est clair que l'ASTNO doit revoir et, le cas échéant, modifier les politiques qu'elle choisit d'appliquer.

Il incombe aux dépositaires de renseignements sur la santé, en vertu de l'article 156 de la *Loi sur les renseignements personnels sur la santé*, de décider de suivre ou non une recommandation formulée dans un rapport d'examen du commissaire. L'ASTNO doit évaluer la recommandation (et la politique en question) et déterminer si elle va suivre la recommandation ou non. Le fait de renvoyer une recommandation au Ministère pour qu'il l'examine ne décharge pas l'ASTNO de la responsabilité qui lui incombe en vertu du paragraphe 156(1) de prendre une décision : cela revient en fait à ne pas prendre de décision. En vertu du paragraphe 156(2), aucune décision n'est réputée être une décision de ne pas suivre la recommandation.

### Rapport d'examen 20 — LRPS 35

Il s'agissait de l'examen d'une demande d'accès à des renseignements sur l'employé ou les employés qui avai(en)t consulté les renseignements personnels sur la santé du requérant. Le requérant a demandé un relevé d'activité (RA), comme le prévoit l'article 8 du *Règlement sur les renseignements sur la santé,* qui est un « rapport préparé par un dépositaire de renseignements médicaux à l'égard des renseignements personnels sur la santé d'un particulier ». Le RA dresse la liste des utilisateurs qui ont accédé aux renseignements personnels sur la santé d'une personne, les dates et heures d'accès, et les informations qui ont été ou auraient pu être consultées. Le requérant pensait que certains renseignements personnels sur la santé (RPS) de nature délicate avaient été conservés sous forme de dossier papier, « en silo » dans une unité de soins de santé spécialisée. Contrairement à ce qui avait été promis, le requérant a appris par la suite qu'une partie des RPS avait été transférée dans le système de dossiers médicaux électroniques (DME) et

qu'elle était alors accessible à toute personne disposant des droits d'accès appropriés à ce type d'information. Le 19 mai 2019, le requérant a demandé des renseignements sur les DSP qui se trouvaient maintenant dans le DME, qui les y avait mis et qui les avait consultés.

Le requérant n'était pas satisfait du RA produit en réponse et a demandé un examen de la part du Commissariat. Le requérant a fait part de préoccupations supplémentaires concernant le respect des délais de réponse, l'absence de réponse écrite et le caractère suffisant de la réponse. Finalement, devant l'insistance du requérant, l'ASTNO a fourni des informations supplémentaires qui, avec le RA, ont répondu à la plupart des questions du requérant. Le 7 octobre 2019, la commissaire a informé l'ASTNO qu'elle entreprenait un examen.

Le rapport contenait sept recommandations. Quatre d'entre elles ont été acceptées et portent sur des questions de procédure : la nécessité de veiller à ce que les demandes d'accès soient traitées dans les délais prévus, par écrit et avec le contenu applicable à la demande. Trois des recommandations n'ont pas été acceptées.

*Recommandation n$^{o}$ 4 : Que l'ASTNO récupère les rapports d'activité (RA) directement dans le DME afin d'éviter les transferts, les manipulations et les retards inutiles.*

Le RA est défini à l'article 8 du *Règlement sur les renseignements personnels sur la santé*, et le paragraphe 8(2) précise que c'est le dépositaire de renseignements sur la santé qui doit « traiter la demande » d'un particulier en vertu de la partie 5 de la Loi. L'ASTNO a dépassé le délai imparti pour produire le RA en vertu de la partie 5 de la Loi.

Dans la pratique, l'ASTNO ne produit pas directement les RA, mais demande au Ministère de le faire. Ce processus induit parfois un retard et peut parfois avoir pour conséquence que le RA ne fournisse pas les informations demandées. La raison pour laquelle l'ASTNO ne récupère pas directement les RA n'est pas claire, mais le fait que le Ministère le fasse pour l'ASTNO ne dispense pas l'ASTNO de son obligation de produire les informations demandées dans les délais légaux[7]. Selon le règlement, la production d'un RA dans cette situation relève de la responsabilité de l'ASTNO, et non de celle du Ministère. L'ASTNO a déclaré qu'elle transmettrait la recommandation au Ministère et « engagerait des discussions sur cette question ».

*Recommandation n$^{o}$ 5 : Que l'ASTNO prenne des mesures pour voir si le DME peut être reconfiguré pour saisir des renseignements plus détaillés afin de mieux répondre aux exigences énoncées dans la législation sur les RA, notamment en réduisant au minimum les incohérences et les lacunes dans les détails.*

L'ASTNO n'a pas accepté cette recommandation, indiquant à nouveau que le DME était sous la responsabilité du Ministère et qu'elle fournirait au Ministère la recommandation et engagerait des discussions sur cette question. Le Ministère semble conserver un grand contrôle sur

[7]En général, en vertu du paragraphe 101(1) de la LRPS, le dépositaire de renseignements sur la santé doit répondre par écrit à une demande d'accès dans un délai de 30 jours. En vertu de l'article 103, si l'accès aux informations doit être autorisé et qu'une copie n'est pas fournie avec la réponse, le dépositaire de renseignements sur la santé dispose d'un délai supplémentaire de 30 jours pour fournir une copie ou permettre l'accès d'une autre manière.

l'utilisation et le fonctionnement du DME, et il semble que l'ASTNO ne puisse pas, de manière indépendante, utiliser pleinement le DME ou y apporter des modifications. Cependant, la recommandation était « de prendre des mesures pour voir si le système de DME peut être reconfiguré ». La déclaration de l'ASTNO selon laquelle elle engagera des discussions sur cette question avec le Ministère constitue une acceptation de la recommandation telle qu'elle est formulée.

*Recommandation nº 7 : Que l'ASTNO examine le contenu des brochures fournies au requérant sur la protection de la vie privée et l'accès à l'information et s'assure que ce qui est écrit est correct et souligne toute divergence entre les informations contenues dans les brochures et les exigences réelles de la législation.*

Avec la réponse écrite officielle à la demande d'accès à l'information du requérant, l'ASTNO a fourni à celui-ci quelques brochures produites par le Ministère sur la façon dont les renseignements personnels sont protégés, notamment dans les dossiers médicaux électroniques. Le requérant s'est inquiété du fait que certaines affirmations faites dans les brochures ne correspondaient pas à son expérience.

La recommandation nº 7 n'a pas été acceptée; là encore, l'ASTNO a indiqué que la recommandation relevait de la responsabilité du Ministère, mais a également promis de transmettre la recommandation au Ministère. Lors de l'examen, le commissaire a noté que les brochures parlent de la capacité de fournir un accès rapide à des dossiers tels que le RA et indiquent comment les systèmes de santé électroniques protégeront la vie privée des patients et leur permettront de contrôler leurs renseignements personnels sur la santé et d'y avoir accès. Les allégations annoncées ne correspondaient pas à l'expérience du requérant et la recommandation visait à encourager le réexamen du contenu des brochures et leur modification, le cas échéant.

Bien que les brochures soient des produits sous le contrôle du Ministère, l'ASTNO est le dépositaire d'informations sur la santé qui distribue les brochures. Si les brochures contiennent des inexactitudes majeures, il faut alors résoudre rapidement le problème. Le fait qu'il en soit l'auteur ne fait pas de la distribution de ces brochures une question relevant uniquement du Ministère. Bien qu'il soit clairement bénéfique pour le Ministère d'être informé de la recommandation, l'ASTNO devrait examiner elle-même si les informations contenues dans les brochures sont exactes avant de les distribuer.

# Tendances et enjeux

## Passeport vaccinal

Alors que nous sortons de la pandémie de COVID-19 et que les arrêtés de santé publique deviennent moins restrictifs, les gouvernements des Territoires du Nord-Ouest et d'ailleurs explorent des options permettant aux personnes de démontrer qu'elles ont reçu le vaccin contre le COVID-19. Il ne s'agit pas seulement de fournir aux personnes qui en font la demande une copie de leur dossier de vaccination, mais aussi de s'attendre à ce que les personnes doivent prouver leur statut vaccinal par une certification ou une autre garantie d'authenticité.

Le concept du passeport vaccinal repose sur l'idée que les personnes qui ont été vaccinées présentent un risque moindre pour la santé publique et que certaines restrictions peuvent raisonnablement être assouplies envers ces personnes. Les voyageurs auront probablement besoin d'une certaine forme de certification de vaccination pour faciliter leur voyage et pour réduire ou éliminer l'obligation de s'isoler à leur retour aux Territoires du Nord-Ouest. Ces documents contiennent des renseignements personnels sur la santé qui sont régis par la *Loi sur les renseignements personnels sur la santé.* Le passeport vaccinal est proposé comme une mesure susceptible de faciliter les voyages, de réduire les restrictions sur les rassemblements sociaux et d'accélérer la reprise économique par une plus grande participation aux activités de la société. Si les passeports vaccinaux peuvent offrir un avantage public substantiel, ils empiètent également sur la vie privée et les libertés civiles et ne devraient être utilisés qu'après mûre réflexion.

Les commissaires à la protection de la vie privée fédéral, provinciaux et territoriaux ont publié une déclaration commune le 19 mai 2021[8] soulignant plusieurs problèmes potentiels causés à la vie privée par les passeports vaccinaux. Qu'il s'agisse d'un voyage international ou d'un voyage au Canada, ces documents exigent nécessairement l'utilisation et la divulgation de renseignements personnels sur la santé régis par la *Loi sur les renseignements personnels sur la santé*. La déclaration commune invite les gouvernements à adhérer au principe de « Privacy by Design » (conception respectant la vie privée) et à collaborer avec les commissaires à la protection de la vie privée pour faire en sorte que les renseignements personnels soient accessibles et utilisés de manière appropriée et qu'ils soient par ailleurs raisonnablement protégés. Le CIPVP a rencontré à ce sujet des fonctionnaires du ministère de la Santé et des Services sociaux ainsi que le directeur de l'information et prévoit d'autres consultations sur cette question dans les mois à venir.

[8] https://priv.gc.ca/en/opc-news/speeches/2021/s-d_20210519/.

## Effets de la COVID-19 sur l'accès à l'information et la protection de la vie privée

La pandémie a affecté de nombreux aspects des opérations gouvernementales. Les services gouvernementaux ont connu des retards et des interruptions dans certaines régions.

En juin 2020, le législateur a adopté une loi[9] permettant d'alléger plusieurs obligations temporelles, mais pas les délais de réponse précisées en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* ou de la *Loi sur les renseignements personnels sur la santé.* Malheureusement, il a été porté à l'attention du Commissariat à l'information et à la protection de la vie privée que, dans un certain nombre de cas, certains organismes publics n'avaient pas rempli leur obligation de répondre aux demandes d'accès à l'information dans les délais prévus par la LAIPVP ou la LRPS. La LAIPVP accorde aux organismes publics un délai de 30 jours pour répondre à une demande, mais permet également aux organismes publics de profiter d'un délai supplémentaire raisonnable. Dans plusieurs cas, les organismes publics ont donné des avis de deux ou plusieurs prolongations de délai de plus de 30 jours et n'ont toujours pas fourni les documents demandés. Parfois, aucun avis de prolongation de délai n'a été fourni, ce qui équivaut à un refus présumé 30 jours après le dépôt de la demande.

En raison de l'incidence des longs délais de réponse aux demandes d'accès, le Commissariat a commencé à intervenir de manière officieuse et à inviter les organismes publics à fournir les documents demandés comme l'exige la législation. L'initiative a été fructueuse dans certains cas, mais a également servi à indiquer à quel point les processus d'accès à l'information sont dépourvus en ressources dans certains ministères. Les retards dans le traitement des demandes d'accès ont également révélé des problèmes de gestion des dossiers, notamment d'organisation et de gestion des systèmes d'information et de messagerie électronique. Les retards ont aussi révélé l'enjeu auquel les organismes publics sont confrontés pour la rétention d'un effectif suffisant, compétent et formé, qui comprend les systèmes d'information et d'archivage des organismes publics, y compris les anciens systèmes papier.

Si la nécessité de maintenir les services gouvernementaux « de base » est manifeste, j'ai le sentiment que les fonctions d'accès à l'information et de protection de la vie privée sont considérées par certains acteurs du gouvernement comme ne faisant pas partie de ce « noyau » de services. Le fait que le législateur n'ait accordé aucun allègement des obligations prévues par la LAIPVP ou la LRPS indique clairement au personnel gouvernemental que l'accès à l'information et la protection de la vie privée sont en fait des fonctions essentielles du gouvernement.

Les organismes publics expliquent souvent ce retard par le fait que la COVID-19 a imposé des charges imprévues au personnel, à tel point qu'il n'a pas été possible de respecter les délais légaux. Il ne fait aucun doute que la pandémie a causé des problèmes à tous et qu'elle a obligé de nombreux employés du gouvernement à travailler à distance, souvent depuis leur domicile. Cette situation a entraîné des difficultés d'ordre pratique dans la fourniture des services gouvernementaux. Il ne fait aucun doute qu'il a été plus difficile de répondre aux demandes

[9]Projet de loi 10 : *Loi modifiant temporairement les délais prévus par la loi (mesures résultant de la pandémie de la COVID-19).* Adoptée le 15 juin 2020.

d'accès à l'information sans que l'on dispose sur-le-champ des installations et des systèmes d'information habituels.

Les délais peuvent également avoir été affectés lorsque certains employés se sont vu attribuer de nouveaux rôles ou des tâches supplémentaires liées à la réponse à la pandémie. Ces raisons, ainsi que d'autres, qui expliquent les retards dans le service sont compréhensibles dans le contexte de personnes travaillant dans un système dont le personnel et les ressources sont limités. Toutefois, les obligations légales d'un organisme public *en tant qu'institution* et les obligations du responsable d'un organisme public sont restées inchangées. Le retrait ou la réaffectation des ressources ont peut-être placé la bureaucratie dans une position où elle a contré l'intention du législateur pour le respect des exigences de la LAIPVP et de la LRPS. Cette situation a causé un stress important à certains employés qui tentaient de satisfaire aux exigences de la loi; des tâches pour lesquelles ils manquaient parfois de ressources et, dans certains cas, n'étaient pas correctement formés. Comme on pouvait s'y attendre, le résultat n'a pas été satisfaisant et pourrait bien avoir contribué à l'augmentation du nombre de demandes de révision. Le commissaire reconnaît les efforts déployés par le personnel des organismes publics pour servir la population dans ces circonstances difficiles et encourage ces organismes à consacrer les ressources nécessaires pour qu'à l'avenir, il y ait suffisamment de personnel correctement formé et équipé pour fournir les services d'accès à l'information prévus par la loi.

Le rapport annuel de l'année dernière reconnaissait que la réponse à la pandémie avait entraîné la collecte d'un grand nombre de renseignements personnels et de renseignements personnels sur la santé pour gérer l'isolement de voyageurs et des personnes ayant contracté la maladie ou courant le risque de la contracter en raison d'un contact avec des personnes porteuses. Le CIPVP a été averti de plusieurs atteintes importantes à la vie privée survenues à la suite d'erreurs d'utilisation du courrier électronique par le Secrétariat pour la COVID-19. À la mi-mars, des fonctionnaires du ministère de la Santé et des Services sociaux ont indiqué qu'une trentaine d'atteintes à la vie privée s'étaient produites au cours de l'année écoulée, dont un grand nombre étaient liées au Secrétariat pour la COVID-19. Ce qui est très préoccupant, c'est qu'aucun signalement de ces atteintes n'a été envoyé au Commissariat lorsque les atteintes ont été confirmées, malgré les exigences de la Politique sur les atteintes à la vie privée du Ministère et de la LRPS. Des enquêtes sont en cours et le commissaire compte aborder cette question dans le rapport annuel de l'année prochaine.

Le Secrétariat pour la COVID-19 a été une réponse à une urgence de santé publique sans précédent. La protection de la confidentialité des renseignements personnels sur la santé fait partie intégrante de la réponse et est prescrite par la loi. Le respect de la vie privée exige une communication claire, une politique et des procédures établies en la matière ainsi qu'une formation adéquate du personnel, ce qui n'est pas hors des capacités du ministère de la Santé et des Services sociaux ou, par extension, du Secrétariat pour la COVID-19. La Politique sur les atteintes à la vie privée doit s'appliquer partout dans l'administration et ne doit pas être compromise, sauf si l'intention du législateur en est clairement exprimée dans la loi.

Le commissaire félicite les organismes publics et les dépositaires de renseignements sur la santé qui signalent les atteintes à la vie privée au Commissariat, en particulier ceux qui l'ont fait dans les délais impartis. Il est clair que les atteintes à la vie privée sont trop souvent causées par des employés qui manquent de ressources ou qui n'ont pas reçu de formation sur les politiques et les procédures régissant la protection de la vie privée ou qui ne les connaissent pas. Une formation complète et régulière sur la protection de la vie privée est souvent recommandée par le commissaire comme moyen d'éviter la répétition d'atteintes à la vie privée, et ce type de recommandation est souvent accepté par les organismes publics. Une formation accrue et de meilleure qualité pour le personnel est un progrès évident. Pourtant, entre les différents ministères et agences assujettis à la LAIPVP et à la LRPS, on constate de grandes variations dans la sensibilisation aux questions de protection de la vie privée et dans les compétences pour répondre aux atteintes à la vie privée. Il ne fait aucun doute qu'il peut être difficile, sur le plan logistique, de fournir une formation complète, régulière et coûteuse en ressources financières et humaines. Toutefois, la protection de la vie privée n'est pas une option ou un « complément » aux principaux objectifs et responsabilités d'un organisme public : elle est fondamentale. La protection de la vie privée exige un niveau approprié de ressources et le soutien des directions de tous les ministères et organismes.

La diffusion élargie des politiques et des procédures applicables peut aussi être utile : d'une manière générale, les employés du gouvernement, le CIPVP et le public devraient disposer d'un accès facile à ce type de documents sur Internet. Ainsi, à la suite d'une recommandation du rapport d'examen 20-LRPS 26, l'ASTNO a accepté de créer un site Web pour mettre ces politiques à la disposition du personnel. Dans le rapport d'examen 20-LRPS 21, l'ASTNO a accepté la recommandation de publier sur son site Web la Politique sur les renseignements stockés et transférés à l'aide des outils électroniques des services de santé et des services sociaux. La publication des politiques est un bon pas vers un gouvernement plus ouvert et transparent.

### *Entrée en vigueur des modifications de la LAIPVP*

Les modifications apportées à la *Loi sur l'accès à l'information et la protection de la vie privée*, qui devraient entrer en vigueur à l'été 2021, amènent plusieurs changements importants :

- Un certain nombre d'éclaircissements sur les exemptions de divulgation de certains types de documents, y compris les dossiers qui peuvent révéler des informations confidentielles du Conseil exécutif ou du Conseil de gestion financière.
- Certaines sections traitent des dossiers relatifs aux enquêtes sur le lieu de travail et aux évaluations des employés ainsi que des dossiers sur les intérêts commerciaux.
- Une nouvelle disposition de « primauté de l'intérêt public » oblige le responsable d'un organisme public à divulguer des informations sur le risque de préjudice important pour l'environnement ou pour la santé et la sécurité du public.

- Obligation d'informer les personnes en cas d'atteintes à leur vie privée qui présentent un risque réel de préjudice important. Le commissaire doit être informé si une atteinte à la vie privée est importante.
- Dans le cadre de l'examen des réponses aux demandes d'accès à l'information et des atteintes à la vie privée, le commissaire aura compétence pour rendre des décrets plutôt que de formuler des recommandations.
- Lorsqu'un organisme public élabore un programme ou un service commun ou intégré, les évaluations des répercussions sur la vie privée devront être soumises au commissaire à l'information et à la protection de la vie privée pour examen et formulation d'observations.
- Comme il est indiqué ci-dessous, un certain nombre de changements ont été apportés aux délais et aux processus d'examen.

Les délais prévus par la LAIPVP pour les examens des réponses aux demandes d'accès à l'information ou des atteintes à la vie privée ont été quelque peu raccourcis, ce qui fait en sorte que les organismes publics disposent de moins de temps pour fournir des documents et fournir des observations pendant l'examen. Souvent, les organismes publics ne fournissent pas leurs observations en temps voulu, et des prolongations de délai sont demandées fréquemment. Maintenant que les examens doivent être réalisés dans un délai plus court, ces accommodements ne peuvent plus être invoqués.

Toutes les parties concernées devront s'assurer qu'elles consacrent suffisamment de ressources à la réalisation les examens dans les délais réglementaires prévus. Il ne serait pas dans l'intérêt du public ni dans l'esprit des lois que le commissaire procède à des examens sans bénéficier d'observations formulées adéquatement par les organismes publics.

Un autre changement apporté dans les délais fait en sorte que les organismes publics qui répondent aux demandes d'accès à l'information ne pourront désormais prolonger le délai de réponse qu'une seule fois de leur propre chef. Si une autre prolongation est nécessaire, l'organisme public devra d'abord demander l'autorisation du commissaire. Il s'agit d'un changement important : l'organisme public devra justifier la prolongation de délai dès le départ, et le commissaire aura une nouvelle fonction décisionnelle à remplir en vertu de la LAIPVP. Il ne s'agit pas d'un processus d'approbation automatique : la Loi exige que le commissaire procède à un examen de la demande de prolongation du délai et qu'il n'autorise une telle prolongation que pour les motifs énoncés au paragraphe 11(1). Si le passé est une indication de l'avenir, il est raisonnable de s'attendre à ce que les organismes publics demandent fréquemment des prolongations de délai.

Depuis mars 2021, le nouveau Bureau de l'accès à l'information et de la vie privée (BAIVP) du ministère de la Justice joue officiellement le rôle de coordonnateur des demandes d'accès à l'information pour un certain nombre d'organismes publics. La centralisation de certaines fonctions d'accès à l'information est réellement prometteuse d'amélioration dans la rapidité et la qualité des réponses aux demandes d'accès aux documents gouvernementaux déposées par le public. Il est trop tôt pour faire des commentaires, sinon que la communication entre le BAIVP et

le CIPVP a été empreinte d'ouverture et de collaboration. Bien que cela risque d'être une évidence, il convient de préciser que de veiller à ce que le BAIVP maintienne sa cohorte de personnel formé et expérimenté aidera grandement les organismes publics à remplir leurs obligations en vertu de la Loi. Cela devrait, en conséquence, limiter ou éviter la tenue d'examens ultérieurs par le CIPVP. Faire les choses correctement dès la première fois est sans aucun doute la meilleure approche.

Conformément à la Politique de protection de la vie privée 82.10 du GTNO, les évaluations des répercussions sur la vie privée (ERVP) doivent être soumises au commissaire pour examen et formulation d'observations lorsque des propositions de « programmes ou de services communs ou intégrés » sont élaborées, ce qui deviendra une exigence légale lorsque les modifications apportées à la LAIPVP entreront en vigueur. La LRPS exige déjà une ERVP lorsqu'un dépositaire de renseignements sur les soins de santé propose un changement, un nouveau système d'information ou une nouvelle technologie de communication. Les pratiques optimales exigent que les évaluations des répercussions sur la vie privée soient préparées dès les premiers stades de l'élaboration des projets afin que l'on puisse assurer que les questions associées à la protection de la vie privée sont correctement prises en considération dans la conception du projet. La Politique de protection de la vie privée précise entre autres qu'une ERVP doit être soumise au commissaire pour examen et formulation d'observations dès les premières étapes des processus d'élaboration, et le paragraphe 42.1(4) de la LAIPVP exige qu'un avis soit envoyé au commissaire dès les premières étapes de l'élaboration d'un programme ou d'un service commun ou intégré. L'expérience acquise avec certaines ERVP soumises dans le cadre de la LRPS à un stade tardif du processus d'élaboration d'un projet, ou même à la fin a clairement démontré qu'il fallait utiliser les ERVP au début du processus d'élaboration.

## Atteintes à la vie privée aux termes de la *Loi sur les renseignements personnels sur la santé*

Le rapport annuel de l'année dernière indiquait que la plupart des atteintes à la vie privée signalées émanaient de l'Administration des services de santé et des services sociaux des TNO (ASTNO). Cela peut sans doute être attribué au fait que l'ASTNO dispense la plupart des services de santé aux Territoires du Nord-Ouest [10] et à l'amélioration de la capacité de l'ASTNO à reconnaître les atteintes à la vie privée lorsqu'elles se produisent et à y réagir de manière appropriée. Le Commissariat a constaté que toutes les autorités sanitaires ont redoublé d'efforts pour signaler les cas d'atteinte à la vie privée, ce qui mérite d'être souligné.

Sur les 66 signalements d'atteinte à la vie privée reçus en vertu de la LRPS au cours du dernier exercice financier, un nombre inquiétant concernait des erreurs dans l'utilisation de télécopieurs pour communiquer des renseignements personnels sur la santé. Pour réitérer l'avis de l'ancienne commissaire, les dépositaires de renseignements sur la santé devraient cesser d'utiliser des

[10] L'ASTNO dispense des services de santé et des services sociaux dans toutes les régions, à l'exception de celles de Hay River, qui est desservie par Administration des services de santé et des services sociaux de Hay River, et des communautés tłı̨chǫ de Behchokǫ̀, Gamètì, Whatì et Wekweètì, lesquelles sont desservies par l'Agence de services communautaires tłı̨chǫ.

télécopieurs pour transmettre des renseignements personnels sur la santé. En réponse au rapport annuel 2018-2019 de la commissaire, le rapport 5-19(2) du Comité permanent des opérations gouvernementales a recommandé que le GTNO élabore et mette en œuvre un plan pour mettre fin à l'utilisation des télécopieurs dans le secteur de la santé et des services sociaux. Le GTNO a appuyé cette recommandation et a indiqué que le ministère de la Santé et des Services sociaux préparait un plan pour améliorer la compréhension de l'utilisation de la télécopie dans l'ensemble du système de santé et de services sociaux et pour continuer à travailler à la réduction du recours à ce moyen de communication. Le CIPVP attend avec impatience l'occasion d'examiner ce plan.

La lenteur avec laquelle les atteintes sont signalées demeure un point préoccupant. L'article 87 de la LRPS exige que les dépositaires de renseignements sur la santé émettent un avis lorsqu'il y a utilisation ou divulgation non autorisée de renseignements personnels sur la santé pour la personne touchée et le commissaire dès que cela est possible. La Politique sur les atteintes à la vie privée du ministère de la Santé et des Services sociaux, qui s'applique au Ministère et à toutes les autorités responsables des services de santé et des services sociaux, exige également un signalement rapide. Néanmoins, il arrive malheureusement trop souvent que l'avis d'atteinte à la vie privée soit reçu des semaines, des mois, voire dans certains cas plus d'un an après que le dépositaire de renseignements sur les soins de santé a été informé de l'incident. Parfois, l'avis est fourni en même temps ou même dans le même document que le rapport final sur l'atteinte fourni au commissaire, plusieurs mois après la confirmation de l'incident.

Les avis doivent être envoyés rapidement. Tout d'abord, la personne faisant l'objet d'une atteinte à la vie privée a le droit d'être avertie de l'utilisation ou de la divulgation non autorisée de ses renseignements personnels sur sa santé. Deuxièmement, l'avis informe les personnes de leur droit de demander un examen au commissaire à l'information et à la protection de la vie privée. Sans ces avis, de nombreuses personnes ne seraient pas au courant des recours judiciaires qui s'offrent à elles. Troisièmement, le commissaire doit être informé pour exercer sa fonction de surveillance indépendante. L'article 87 de la *Loi sur les renseignements personnels sur la santé* exige qu'un avis soit envoyé à la personne concernée et au commissaire dès qu'il est raisonnablement possible de le faire. Le cadre politique et législatif actuel fournit l'orientation appropriée aux dépositaires de renseignements sur la santé, mais le signalement des atteintes à la vie privée est néanmoins fréquemment retardé, souvent sans justification. Le CIPVP demeurera attentif à cette question.

## Réponses rapides au CIPVP

Le respect des délais est une question importante tant en vertu de la LAIPVP que de la LRPS. Si un examen est demandé par une personne en vertu de la LRPS, le commissaire doit faire de son mieux pour conclure l'examen dans un délai de 120 jours civils[11]. Lorsque les modifications apportées à la LAIPVP entreront en vigueur, le délai pour effectuer un examen passera de 180 jours civils à 90 jours ouvrables[12].

Après avoir reçu un avis d'atteinte à la vie privée en vertu de la *Loi sur les renseignements personnels sur la santé*, le Commissariat attendra généralement de recevoir un rapport final du dépositaire des renseignements sur la santé. Selon ce qui est révélé et si une demande d'examen a été déposée, le commissaire peut entreprendre un examen. L'exercice peut exiger la recherche de dossiers et de déclarations supplémentaires auprès du dépositaire des renseignements sur la santé. Ce processus nécessite parfois un suivi répété.

Une fois que le commissaire a entrepris un examen en vertu de la *Loi sur la protection des renseignements personnels*, le paragraphe 153(2) exige que « le dépositaire de renseignements sur la santé produise les copies des documents requis pour examen par le commissaire à l'information et à la protection de la vie privée dans les 14 jours suivant la réception d'une demande en ce sens. » [*Nous insistons sur ce point.*] Souvent, ce délai de réponse n'est pas respecté, même si les dépositaires de renseignements sur la santé n'ont pas le pouvoir discrétionnaire de négliger ce délai et que le commissaire n'a pas la compétence pour prolonger le délai de réponse. Le législateur a déterminé que l'intérêt public est mieux servi par la production rapide de documents à la demande du commissaire. Les dépositaires de renseignements sur la santé devront prendre les mesures requises pour s'assurer qu'ils sont en mesure d'agir dans les délais établis par la Loi.

## Réponses rapides aux demandes d'accès à l'information

Le CIPVP a reçu plusieurs plaintes concernant les délais de réponse aux demandes d'accès à l'information en vertu de la LRPS. La Loi permet actuellement aux organismes publics de prolonger le délai de réponse à une demande pour une période raisonnable dans certaines circonstances. Dans la pratique, les organismes publics prolongent souvent le délai plus d'une fois pour la même demande d'accès. L'envoi d'un avis au requérant exposant la raison de la prolongation et d'un conseil concernant son droit de demander un réexamen de la prolongation est une étape clé de la procédure de prolongation.

Dans plusieurs cas, il y a eu des retards importants dans la réponse des organismes publics à une demande d'accès à l'information; dans certains cas, l'organisme public a finalement fourni la réponse substantielle après que le Commissariat soit intervenu. Dans certains de ces cas, cela a amené le requérant à retirer sa demande d'examen. Dans d'autres cas, nous avons eu

[11]Article 149 de la Loi sur les renseignements personnels sur la santé.

[12]Paragraphe 31(3) de la Loi sur l'accès à l'information et la protection de la vie privée.

connaissance de manquements à l'obligation de répondre qui ont duré des mois sans que le requérant soit informé d'une prolongation du délai et sans réponse substantielle, laissant ainsi le requérant sans autre choix que de demander la poursuite de l'examen.

Bien que les modifications apportées à la LAIPVP ne constituent pas la garantie d'une réponse rapide, les organismes publics ne pourront désormais s'accorder qu'une seule prolongation raisonnable du délai. Toute prolongation supplémentaire ne sera possible que si elle est autorisée par le commissaire. Le non-respect délibéré des conditions d'une telle autorisation pourrait éventuellement entraîner l'imposition de sanctions en vertu de l'alinéa 59(2)d) de la Loi. Le nouveau Bureau de l'accès à l'information et de la vie privée du ministère de la Justice sera sans doute d'une grande aide pour assurer le respect des nouveaux délais, mais certains organismes publics n'ont pas désigné ce bureau en tant que coordonnateur de l'accès à l'information et de la protection des renseignements personnels. Et, nonobstant les modifications apportées à la Loi et le nouveau Bureau de l'accès à l'information et de la protection des renseignements personnels, les responsables des organismes publics demeurent les personnes qui ont la responsabilité de répondre aux demandes d'accès à l'information dans les délais fixés par la Loi. Les responsables devront s'assurer que leurs directions et agences sont prêtes pour les changements.

## Enregistrements audio et vidéo mobiles personnels

L'utilisation des appareils mobiles personnels a fait l'objet d'une étude minutieuse dans quelques examens. Le rapport d'examen 20-242 portait sur l'utilisation d'un appareil d'enregistrement mobile personnel pour prendre des séquences vidéo d'un enseignant et d'élèves dans une salle de classe. La vidéo a été créée par un responsable de l'éducation et placée ensuite sur un serveur gouvernemental pour un accès général, apparemment à des fins de formation. Le consentement pour cette collecte, cette utilisation et cette divulgation de renseignements personnels n'a pas été demandé ou obtenu. Au cours de l'enquête du commissaire, un facteur clé est ressorti : l'absence de toute orientation politique concernant l'utilisation de ces appareils personnels sur le lieu de travail. Le ministère de l'Éducation a accepté la recommandation voulant qu'il élabore une politique sur cette question et a indiqué qu'il y donnerait suite en collaboration avec le Bureau de l'accès à l'information et de la vie privée du GTNO.

Dans un autre examen, un conseiller a laissé un appareil mobile en marche et son application de communication audio ouverte, ce qui a eu pour conséquence qu'une conversation confidentielle avec un client a été partagée par inadvertance avec un tiers. Le risque que des renseignements personnels de nature très délicate soient collectés, utilisés ou divulgués sans autorisation est élevé. Étant donné l'omniprésence des appareils personnels de poche dotés d'une capacité d'enregistrement vidéo et audio, il est primordial d'attirer l'attention sur les risques posés pour la protection de la vie privée et de fournir des orientations politiques claires sur leur utilisation par les employés du gouvernement.

# Mot de la fin

Dans notre démocratie représentative, il est primordial que le droit d'accès du public aux documents gouvernementaux soit respecté sous réserve uniquement des exceptions étroites prévues par la Loi. De même, la protection de la vie privée et des renseignements personnels est essentielle si l'on veut que le public se fie au gouvernement. Le temps et les efforts requis pour assurer l'exercice effectif du droit d'accès sont considérables, tout comme le temps et les efforts qu'il faut consentir pour concevoir, planifier et mettre en œuvre des mesures de protection de la vie privée. L'accès à l'information et la protection de la vie privée exigent l'affectation de ressources gouvernementales : ces tâches ne peuvent être accomplies depuis « le coin du bureau ». Il faut disposer d'un effectif formé et expérimenté, disposant de ressources suffisantes et du soutien indéfectible de la direction, pour remplir les responsabilités gouvernementales prévues par la LRPS et la LAIPVP. Les dépositaires de renseignements sur la santé et les organismes publics doivent consentir des investissements et des efforts considérables pour s'acquitter de leurs obligations.

L'intérêt du public pour l'accès aux dossiers gouvernementaux ne montre aucun signe de ralentissement. Les questions entourant la protection de la vie privée devraient également continuer à prendre de l'ampleur, car le gouvernement continue à collecter et à utiliser des renseignements personnels. Le piratage électronique, les rançongiciels et autres logiciels malveillants sont des menaces omniprésentes capables de causer des dommages considérables et de compromettre non seulement la capacité du gouvernement à fournir des services, mais aussi la sécurité des imposantes quantités de renseignements personnels contenues dans les dossiers électroniques. La sécurité des documents gouvernementaux devrait bénéficier d'une planification diligente mettant à profit les évaluations des répercussions sur la vie privée dès les premières étapes de la conception des projets ou des programmes.

Dans un avenir prévisible, la technologie ne remplacera pas les compétences et l'expertise des spécialistes de la protection de la vie privée ou des coordonnateurs de l'accès à l'information travaillant pour des ministères ou des organismes. Il faut donc consacrer des ressources, notamment un effectif qualifié et formé suffisant, pour faire en sorte que le public soit bien servi et que les organismes publics et les dépositaires de renseignements sur la santé soient en mesure de s'acquitter de leurs devoirs et obligations en vertu de la Loi.

# Nous joindre

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

**Téléphone : 1-867-669-0976**
**Sans frais :  1-888-521-7088**
**Téléc. :  1-867-920-2511**

**Courriel : admin@atipp-nt.ca**

**Site Web :  www.atipp-nt.ca**

**Notre bureau est situé au premier étage de l'immeuble Laing à Yellowknife, au coin de l'avenue Franklin et de la 49e Rue; l'entrée se trouve sur l'avenue Franklin.**