Northwest Territories

Annual Report 2021 – 2022

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

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

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

Kīspin ki nitawihtīn ē nīhīyawihk ōma ācimōwin, tipwāsinān.
Cree

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

Ɂerıhtł'ís Dëne Sųłıné yatı t'a huts'elkër xa beyáyatı theɂą ɂat'e, nuwe ts'ën yółtı.
Chipewyan

Edı gondı dehgáh got'ı̨e zhatıé k'ę̨ę̨datł'éh enahddhę nıde naxets'ę̨ edahłí.
South Slavey

K'áhshó got'ı̨ne xədə k'é hederı ɂedı̨htl'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 ᑎᑎᕐᑲᐃᑦ ᐱᔪᒪᒍᕕᒋᑦ ᐃᓄᒃᑎᑐᓕᕐᓯᒪᓗᑎᒃ, ᐅᕙᑦᑎᓐᓄᑦ ᐅᖄᓚᔪᓐᓇᖅᑐᑎᑦ.
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, 2022

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

Dear Mr. Speaker,

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

Your truly,

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

/af

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

Table of Contents

Commissioner's Message Page 1

Financial Report Page 3

Office of the Information and Privacy Commissioner and Enabling Legislation Page 5

- The Access to Information and Protection of Privacy Act
- The Health Information Act
- The Information and Privacy Commissioner

The Year in Review Page 8

- Overview of the Numbers (ATIPPA and HIA)
- Access to Information and Protection of Privacy Act
  - *Review Reports*
  - *Time Extension Requests*
  - *Review of Draft Legislation*
  - *Timelines in ATIPPA*
- Health Information Act
  - *Review Reports*
  - *Increase in Privacy Breaches*
  - *Recurring Issues in Privacy Breaches*
  - *Privacy Impact Assessments*

Interjurisdiction Activity Page 20

Final Thoughts Page 21

Summary of Recommendations Page 22

Contact Us Page 23

Commissioner's Message

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

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

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

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

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

in files opened in the OIPC from 2011/12 to 2019/20.[2] The increasing file load raises questions regarding the efficacy of privacy protection policies and processes governing health information custodians and also raises concerns about the resourcing of access to information and privacy protection functions, both for public bodies and for the OIPC. The increase in new matters is likely due to an increased number of privacy breaches as well as more thorough reporting. I anticipate the number of privacy impact assessments submitted to our office will continue to increase. We will be monitoring the volume and type of new matters going forward.

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

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

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

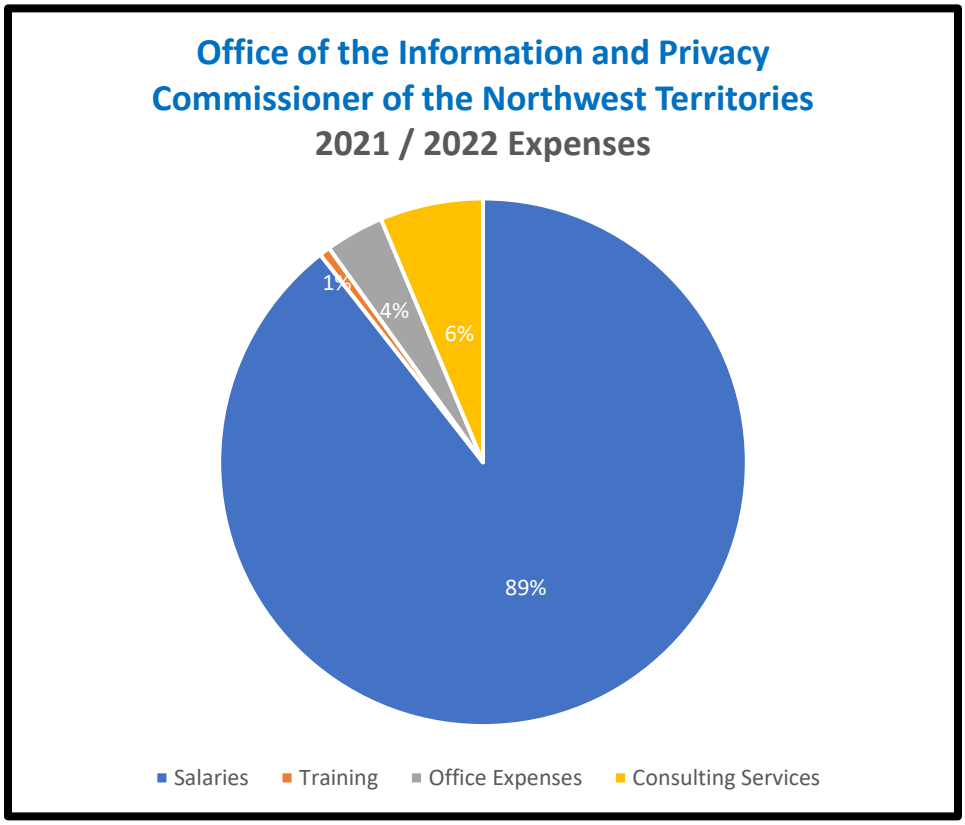
[2] This was identified most recently in the Legislative Assembly's Standing Committee on Government Operations' Report on the Review of the 2020-21 Annual Report of the IPC. See page 2.

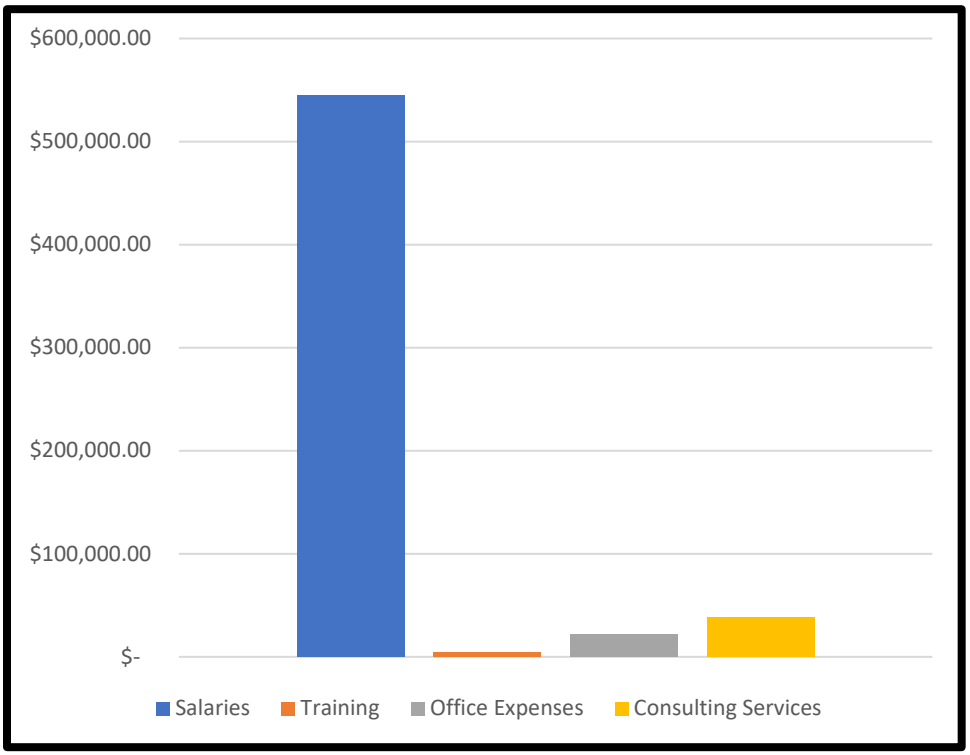
Financial Report

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

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

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


Office of the Information and Privacy Commissioner of the Northwest Territories
2021 / 2022 Expenses
1%
4%
6%
89%
Salaries
Training
Office Expenses
Consulting Services


$600,000.00
$500,000.00
$400,000.00
$300,000.00
$200,000.00
$100,000.00
$-
Salaries
Training
Office Expenses
Consulting Services

Office of the Information and Privacy Commissioner and Enabling Legislation

The Access to Information and Protection of Privacy Act

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

The *ATIPPA* enshrines four key rights and obligations:

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

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

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

[3] *SNWT 1994, c 20.*
[4] Subject to limitations and exceptions set under ATIPPA or other legislation.
[5] No communities have yet been designated.

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

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

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

The Health Information Act

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

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

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

[6] Substantial amendments were passed in SNWT 2019 c.8 and came into force on July 30, 2021.
[7] SNWT 2014, c 2.

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

The Information and Privacy Commissioner

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

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

PIAs have been required under the HIA since it came into force in 2015 and they are now required under the ATIPPA[8] and the GNWT's Protection of Privacy Policy 82.10.[9] In addition to PIA's, the Commissioner may also review and comment on proposed legislation in regard to possible implications for privacy protection or access to government information.

[8] Section 42.1 came into force with the other amendments on July 31, 2021.
[9] This policy has been in place since August 2019.

The Year in Review

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

Overview of the Numbers

Access to Information and Protection of Privacy Act (ATIPPA)

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

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

Health Information Act (HIA)

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

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

Access to Information and Protection of Privacy Act

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

Review Reports

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

Review reports are freely available on-line at https://www.canlii.org/en/nt/ntipc/ .[10]

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

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

[10] Past years' decisions are also available on-line on this free public database.
[11] The Act does not define this term but there are factors to consider set out in subsection 49.9(2).

Time Extension Requests

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

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

Time extensions for third-party consultation

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

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

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

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

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

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

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

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

The Government of the Northwest Territories (GNWT) has created the Access and Privacy Office (APO) to provide support to all GNWT departments[14] to fulfill their ATIPPA obligations. Through this "Centralized Service Model" the GNWT has assigned many of the public bodies' access to information functions to the APO. This promotes and concentrates expertise within that office, helping to bring critical knowledge and experience and efficiency to the access to information process. This appears to be a good service model and my office has already seen the positive effects of this initiative.

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

Although the APO is the designated access to information coordinator[16] for government departments, responding to an access request with the statutory framework remains the public bodies' legal responsibility. I recently examined this issue in a review report addressing an application for an extension based on subparagraph 11(1)(b). [17] I was advised that the APO has been short staffed for the last two years and that the public body had failed to provide its response within the statutory time three times on recent files. The public body was relying on the APO to do its assigned functions, even though it was apparent that the APO did not have the capacity. While each request for authorization must be reviewed on its own merits, it will likely be difficult for a public body to satisfy the requirements for an extension under subsection 11(1)(b) if the public body relies on a unit in another department to do the necessary work, and that unit is not staffed and resourced sufficiently to do that work. In my view, this situation warrants further attention.

[14] And the Northwest Territories Housing Corporation

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

[16] Since October 27, 2020.

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

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

Reviews of Draft Legislation

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

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

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

Timelines in ATIPPA

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

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

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

[18] See section 31(3).

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

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

Health Information Act

Review Reports

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

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

Alternative Solutions

In part, the decrease in the number of reports reflects an increase in the use of alternative approaches to resolving matters. Conducting reviews and issuing review reports with recommendations to the custodian[19] is one process. Another is to work with the health information custodian to address a matter using alternate dispute resolution process [20] or, even less formally, by providing comment and guidance and identifying relevant resources for consideration. This flexible approach continues to be well received by custodians and has led custodians to develop new measures to prevent privacy breaches and to respond better to breaches when they occur. I will continue to use this approach where appropriate.

Responding to Commissioner's Recommendations

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

[19] On request by an individual under Section 134 or on the Commissioner's own initiative under section 137.
[20] Section 138.
[21] Section 156.

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

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

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

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

Increasing Privacy Breaches

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

The following custodians reported breaches this year:

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

[22] https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc28/2020ntipc28.html

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

COVID Secretariat

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

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

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

NTHSSA

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

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

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

[24] See section 87, *Health Information Act*.

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

Recurring Issues in Privacy Breaches

Faxing

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

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

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

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

Vigilance required when using e-Mail

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

[25] For example, see 20-HIA 26 and 20-HIA 27 (CanLII) 2020 NTIPC 23 and 2020 NTIPC 24
https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc23/2020ntipc23.html
https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc24/2020ntipc24.html
[26] See Recommendation #3, pages 6-7 at
https://www.ntassembly.ca/sites/assembly/files/cr_30-192_-_scogo_report_on_the_review_of_the_2020-2021_annual_report_of_the_information_and_privacy_commissio.pdf
[27] See Government of the Northwest Territories Response to Committee Report 5-19(2): Report of the Information and Privacy Commissioner of the Northwest Territories at page 3. Located at:
https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf

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

Paper Records

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

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

Privacy Training

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

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

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

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

Privacy Impact Assessments

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

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

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

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

---

[28] Section 89

[29] Section 175

[30]

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

[31]

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

For example, in a recent review report[32] addressing the protection of confidentiality in the context of a telehealth consultation, my office requested a copy of the PIA for the Telemerge system that replaced the older telehealth system. The request was made twice in writing, but we received no response from NTHSSA. Eventually, the review proceeded on the basis that a PIA had not been completed. The review report recommended that NTHSSA conduct a PIA for the Telemerge system, a system that was replacing the older telehealth system. That recommendation was made on April 29, 2022 and accepted by NTHSSA in a letter dated May 27, 2022. That letter referred to a PIA submitted to my office on May 9, 2022. That PIA was signed by officials between February and June 2021. The PIA states that "The Telemerge migration occurred between the dates of August 13th, 2019, and February 26th, 2020."

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

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

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

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

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

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

[34] See sections 89 and 175 of HIA

[35] See section 42.1 of ATIPPA

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

Interjurisdictional Activity

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

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

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

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

Final Thoughts

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

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

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

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

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

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

Summary of Recommendations

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

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

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

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

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

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

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

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

Contact Us

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

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

Email: admin@oipc-nt.ca

Website: www.oipc-nt.ca

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