

Annual Report 2023-2024



OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
NORTHWEST TERRITORIES



Northwest Territories

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

English

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

French

Kĩspin ki nitawih̄tĩn ē nĩhĩyawih̄k ōma ācimōwin, tipwāsinān.

Cree

Tłjchq yati k'ǽ Di wegodi newq dè, gots'o gonede.

Tłjchq

ʔenht'is Dēne Sųłiné yati t'a huts'elkēr xa beyáyati theʔ ʔat'e, nuwe ts'ēn yółti.

Chipewyan

Edi gondi dehgáh got'je zhatié k'ǽdat'éh enahddhę nide naxets'ę edahlı.

South Slavey

K'áhshó got'jne xədə k'é hederı ʔedjht'é yerınwę nide dúle.

North Slavey

Jii gwandak izhii ginjik vat'atr'ijahch'uu zhit yinothtan ji', diits'at ginohkhii.

Gwich'in

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.

Inuvialuktun

Ĉ'bdĠŋŋ^{sb}Δ^cΛ^cLJΔ^rΔ^cΔ^bŋ^cĈ^{sb}Ŵ^bŴ^b, Đ^cŋ^aĐ^cĐ^{sb}Ĉ^aΔ^{sb}ŋ^c.

Inuktitut

Hapkua titiqqat pijumagupkit Inuinnaqtun, uvaptinnut hivajarlutit.

Inuinnaqtun

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



July 1, 2024

The Honourable Shane Thompson
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, 2023, to March 31, 2024.

Yours truly,

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

/af

Table of Contents

| | |
|---|---------|
| <u>Commissioner's Message</u> | Page 1 |
| <u>Financial Report</u> | Page 4 |
| <u>Office of the Information and Privacy Commissioner and Enabling Legislation</u> | Page 6 |
| <i>The Access to Information and Protection of Privacy Act</i> <i>The Health Information Act</i> The Information and Privacy Commissioner | |
| <u>The Year in Review</u> | Page 9 |
| Overview of the Numbers (ATIPPA and HIA) | |
| <i>Access to Information and Protection of Privacy Act</i> | |
| <u>Review Reports</u> | |
| <u>Time Extension Requests</u> | |
| <u>Delay in Responding to Access Requests – Resourcing the APO</u> | |
| <u>Review of Draft Legislation</u> | |
| <i>Health Information Act</i> | |
| <u>Review Reports</u> | |
| <u>Alternate Resolutions</u> | |
| <u>Responding to Commissioner's Recommendations</u> | |
| <u>A Recommendation Not Accepted</u> | |
| <u>Incidence of Privacy Breaches</u> | |
| <u>Recurring Issues in Privacy Breaches</u> | |
| <u>Privacy Training</u> | |
| <u>Delay in Breach Notification</u> | |
| <u>Privacy Impact Assessments</u> | |
| <u>Interjurisdictional Activity</u> | Page 21 |
| <u>Final Thoughts</u> | Page 22 |
| <u>Summary of Recommendations</u> | Page 23 |
| <u>Contact Us</u> | Page 24 |

Commissioner's Message



I am pleased to provide this year's annual report on the activities of the Office of the Information and Privacy Commissioner. This report is submitted to the Speaker of the Legislative Assembly as required by section 68 of the *Access to Information and Protection of Privacy Act* and section 173 of the *Health Information Act*.

The year was punctuated with events.

- Our new assistant commissioner, Megan Holsapple, joined the office in July 2023. Megan brings to the job a wealth of experience and insight as a former GNWT employee and a passion for the work of the office.
- In mid-August, the office was evacuated on short notice along with most of the City of Yellowknife due to wildfire safety concerns. Work was significantly interrupted during the following three weeks. Evacuation on short notice has nothing to recommend it. At least the city was intact when we returned. Other communities were not so lucky.
- In November, the office moved from the Laing Building to the Northwest Tower – a significant and much-needed improvement in office accommodations!
- In December the Dehcho Divisional Education Council filed a Notice of Appeal of a review report issued November 23, 2023. The report reviewed an unauthorized disclosure of personal information that occurred when the public body disclosed records under section 5.1 of the *Access to Information and Protection of Privacy Act*. Section 5.1 is a new provision, and this was the first instance of a public body relying on it to disclose information. The appeal was discontinued in March 2024 without our office taking a formal step, although not without incurring some legal expense.

There was a moderate decrease in the number of new files this year. We are focusing on reducing the backlog of files and will continue to do so. The goal is to see our office provide reviews within the timelines contemplated by the *Access to Information and Protection of Privacy Act* (ATIPPA) and the *Health Information Act* (HIA).

Some government departments continue to be challenged to respond to access to information requests in a timely manner. My office has seen an increase in the number of requests for review where the public body has not delivered its response in time. Generally, the result is an order requiring the public body to deliver its response forthwith. I am encouraged by the Minister of Justice's commitment in his June 12, 2024, mandate letter, undertaking to respond to access to information requests in a timely manner. Perhaps this will lead to positive change.

We have seen no increase in resources for the Access and Privacy Office, though the need is demonstrable. The Premier has mentioned the issue of resources, and the difficulty public bodies are having in meeting the timelines in the Act.¹ The Premier stated that the Legislative Assembly is "going to conduct a review of the ATIPP Act² and review those timelines because we want to live up to our obligations but we can't set goals for ourselves that are just not achievable with the resources that we have." He also said, "I don't think it's unreasonable to think that setting some more reasonable timelines is on the table."³

I acknowledge the difficult policy choices involved in resourcing the access to information function. These are matters that the legislature will have to wrestle with during the upcoming review of the Act, and I look forward to participating in that review. In my view, lowering the requirements for public bodies is not the best way forward. Adjusting the response timelines without providing more resources to complete the work will not address the problem; it could only provide a temporary reprieve.

Providing timely responses to access requests is demanding in terms of time and skilled personnel – both of which are typically in short supply and require financial resources that are also scarce. Not every problem can be solved by increasing resources; however, some can and the staffing level at the APO is a prime candidate. The Access and Privacy Office (APO) offers centralized efficiency and expertise to assist government departments to respond to access requests, and it offers a simplified "one service window" mode for the public to submit access requests to government departments. The APO has not had an increase in its staff cohort since it assumed its current duties in 2021. Unfortunately, experience since then has demonstrated that government departments are frequently unable to meet the timelines in the Act.

This year my office received 22 requests for review based on a deemed refusal of a government department to provide its response to an access request. Many of these deemed refusals were delays attributable to too many competing demands on APO staff; others were

¹ See Northwest Territories Hansard, February 8, 2024, pages 4, 9, and 19-20.

² Section 74(1) requires the Minister to review the ATIPPA within 18 months of the start of the 20th Assembly.

³ See Hansard, note 1 above.

attributable to delays by the public body itself. In each case, the public body did not apply for an extension of time: relief that is available in certain circumstances.⁴

No doubt, public bodies' resources are limited and responding to access requests may be viewed as an 'add-on' responsibility that takes resources away from a department's core responsibilities. This is not new. In 1990 the Federal Court reflected on this issue:

The Court is quite conscious that responding to such requests is truly "extra work" which is extraneous to the line responsibilities and very raison d'être of government departments and other information-holding organizations of government. But when, as in the *Access to Information Act*, Parliament lays down these pertinent additional responsibilities, then one must comply.⁵ [emphasis added]

The *Access to Information and Protection of Privacy Act* requires a public body to respond to an access request within 20 business days unless the period is extended. This response period is typical across Canada. The challenge is for public bodies to organize themselves to comply with the law. In a free and democratic society that respects the rule of law, this is fundamental.



⁴ These are set out in section 11(1)(a)-(d)

⁵ Justice Muldoon of the Federal Court, Trial Division in *Canada (Information Commissioner) v. Canada (Minister of External Affairs)* [1990] 3 F.C. 514 (F.C.T.D.) in relation to the federal *Access to Information Act*:

Financial Report

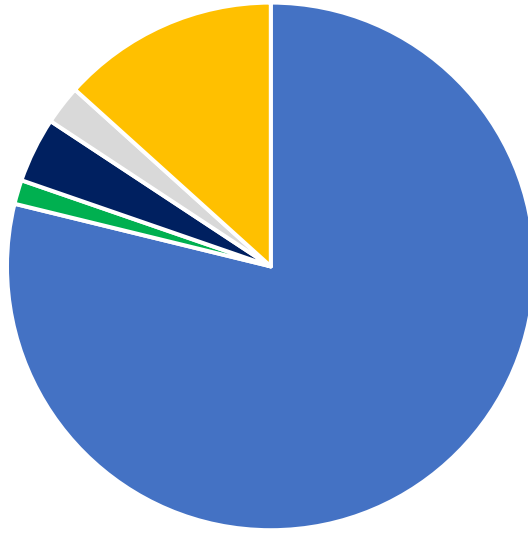
The total amount spent to operate the Office of the Information and Privacy Commissioner (OIPC) of the Northwest Territories for the fiscal year 2023/2024 was \$823,025.55. A detailed breakdown is outlined in the charts below.

Again, the administration of the OIPC budget was uneventful except for the addition of our new office lease payments and the renovations before we could move into the new space. This year's total operating budget was \$ 892,000.00 and we returned \$ 68,974.45 to the Legislative Assembly. There were a few circumstances affecting our finances:

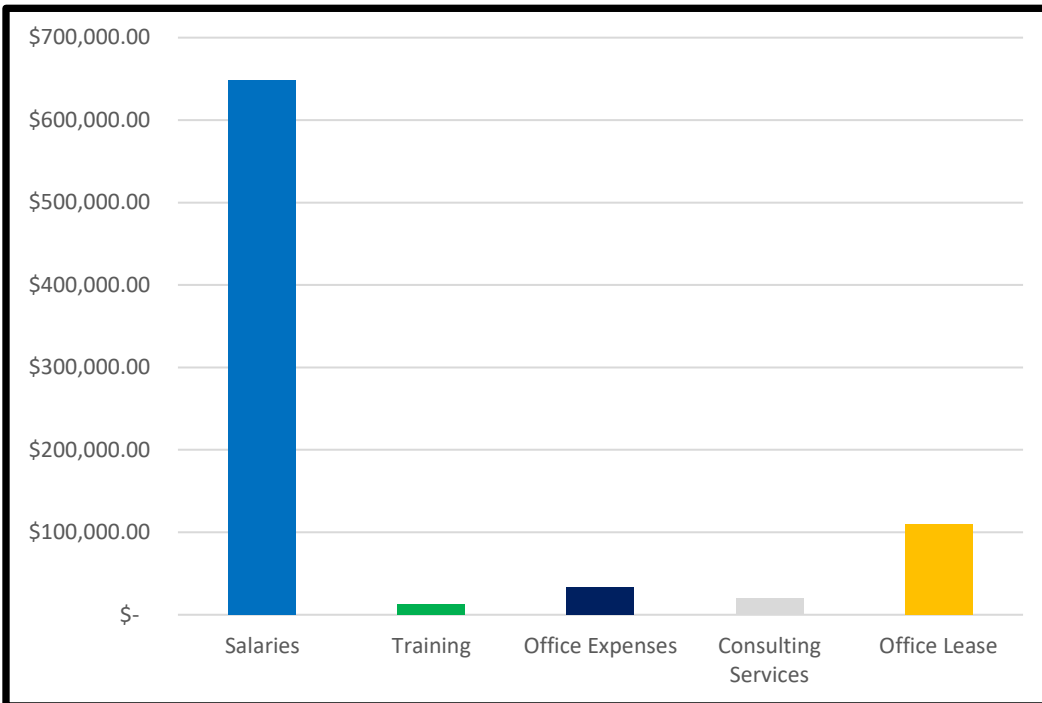
1. The new office space required minor renovations and new telecommunications infrastructure. Renovation was delayed due to the evacuation of August-September, and the lease obligations were not incurred until occupancy commenced on November 1, 2023. Some budget items were reallocated to cover these one-time expenses: budgeted lease payments of April to October 2023, and budgeted salary for the Assistant Commissioner, a position that was vacant from April 1 to July 10, 2023. No extra contributions were required for renovations or moving expenses.
2. Professional development and training for staff is a continuing expense. Our Investigator and Assistant Commissioner were both enrolled in accredited on-line privacy courses.
3. We continue to retain a consultant to assist with reviewing Privacy Impact Assessments. This is a fluctuating source of work-demand, but with the new requirement for privacy impact assessments under the *Access to Information and Protection of Privacy Act*, we expect this to continue to be a significant resource draw.
4. Our office now has four permanent full-time staff.

| Year | Total Expenses | # of Staff |
|-----------|----------------|------------|
| 2019/2020 | \$ 395,144.40 | 1.33 |
| 2020/2021 | \$ 547,168.63 | 2.5 |
| 2021/2022 | \$ 609,279.53 | 3 |
| 2022/2023 | \$ 736,202.84 | 4 |
| 2023/2024 | \$ 823,025.55 | 4 |

Office of the Information and Privacy Commissioner
of the Northwest Territories
2023/2024 Expenses



■ Salaries ■ Training ■ Office Expenses ■ Consulting Services ■ Office Lease



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*⁶ (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*.⁷ With the amendments that came into force in 2021, municipalities may be designated as public bodies by regulation.⁸

The ATIPPA enshrines four key rights and obligations:

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

The *Act* has two fundamental purposes: to provide access 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* establishes the right of the public to access records held by public bodies and outlines a process for members of the public to obtain access to such records. Part 2 governs public bodies' collection, use, and disclosure of individuals' personal information. Amendments to the *Act* that came into force in 2021 provided additional privacy breach response requirements and introduced privacy impact assessment requirements.⁹

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

⁶ SNWT 1994, c 20.

⁷ Subject to limitations and exceptions set under ATIPPA or other legislation.

⁸ No communities have yet been designated.

⁹ Substantial amendments were passed in SNWT 2019 c.8 and came into force on July 30, 2021.

depending on the nature of the review. A public body is required to comply with the Commissioner's order, subject to appeal to the Supreme Court of the Northwest Territories.

Access to information and protection of privacy are both essential to ensure transparency and accountability of government -- vital elements for a healthy and effective democracy. Although access to government records is a legal right, it is not unfettered: there are statutory exceptions -- some mandatory, some discretionary -- that permit public bodies to withhold all or part of some records. Protecting the public's right of access to information and applying the relevant statutory exceptions can involve complex decisions. Independent oversight provides confidence that public bodies apply the *Act* correctly, helping to assure applicants that their rights are being upheld.

The Health Information Act

The *Health Information Act*¹⁰ (*HIA*) governs the collection, use and disclosure of personal health information. It codifies the right of individuals to access their personal health information, the obligation of health information custodians to safeguard individual privacy and ensures that personal health information is available to support the provision of health care services. The *HIA* regulates health information custodians in both the public and the private sectors, including the Department of Health and Social Services, the Northwest Territories Health and Social Services Authority, the Hay River Health and Social Services Authority, the Tłı̄ch̄o Community Services Agency, and private physicians and pharmacists operating in the Northwest Territories.

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

The *HIA* also requires health information custodians to notify affected individuals¹¹ 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.¹² The Commissioner may initiate an investigation of a privacy breach upon the request of an individual who believes their personal health information was collected, used, or disclosed in contravention of the *Act*, or, in appropriate circumstances, the Commissioner may initiate a review independently. After conducting a review, the Commissioner will prepare a report and may make recommendations to the health information custodian. The health information custodian must notify the Commissioner of the

¹⁰ SNWT 2014, c 2.

¹¹ Section 87 of the *Health Information Act*.

¹² Section 87 of the *Health Information Act* and Section 15(2) of the *Health Information Regulations*.

health information custodian's decision to follow or not to follow the recommendation(s) within 30 days of receiving a report. Further, the health information custodian must comply with a decision to follow the Commissioner's recommendation within 45 days of giving notice of the decision to the Commissioner. Applicants who are unsatisfied with a health information custodian's decision regarding a recommendation may appeal the decision to the Supreme Court of the Northwest Territories.

The Information and Privacy Commissioner

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

The Commissioner's powers, duties and functions set out under the *Access to Information and Protection of Privacy Act (ATIPPA)* and the *Health Information Act (HIA)* are carried out through the Office of the Information and Privacy Commissioner (OIPC). The Commissioner's primary functions involve receiving and reviewing complaints about breaches of privacy and about the adequacy of public bodies' responses to access to information requests.

The Commissioner will also review and comment on Privacy Impact Assessments (PIAs) that are submitted to the Office of the Information and Privacy Commissioner. PIAs are generally required when a public body or health information custodian is developing a new system, project, program, or service involving the collection, use or disclosure of personal information or personal health information. PIAs are a key planning tool to ensure that the privacy implications of proposed policies or programs, etc., are considered at an early stage. A PIA helps identify where policies or programs align with legislative requirements and identify gaps or weaknesses that may require resolution *before* implementation. PIAs have been required under the *HIA* since it came into force in 2015, since 2019 under the GNWT's Protection of Privacy Policy 82.10, and since 2021 under the ATIPPA.

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

The Year in Review

The Office of the Information and Privacy Commissioner opened 140 files in the fiscal year 2023/2024.

Overview of the Numbers

Access to Information and Protection of Privacy Act (ATIPPA)

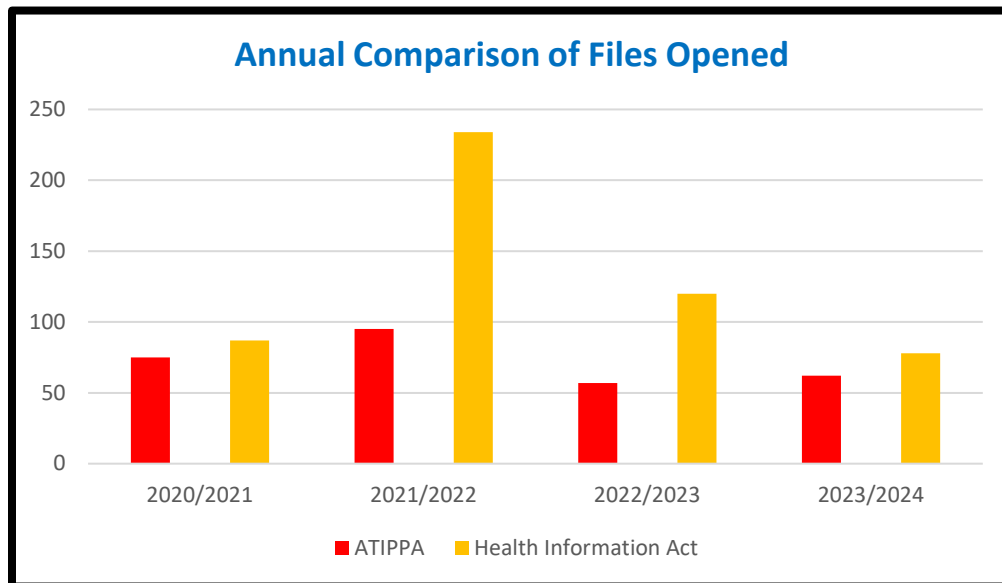
The OIPC opened **62 files** under the *Access to Information and Protection of Privacy Act* between April 1, 2023, and March 31, 2024:

| | |
|---|----|
| Request for Review – Challenging redactions made in access response | 10 |
| Request for Review – Fees, delays, extensions or refused access | 25 |
| Request for Review – Breach of privacy complaint | 5 |
| Request for Review – Correction to records | 1 |
| Request for Time Extension to respond to access request | 9 |
| Notification from Public Body - Breach of privacy | 6 |
| Consultations/Comments – Acts, Bills, PIAs, policies | 3 |
| Miscellaneous, Administrative & OIPC Initiated | 3 |

Health Information Act (HIA)

The OIPC opened **78 files** under the *Health Information Act* between April 1, 2023, and March 31, 2024:

| | |
|--|----|
| Notifications from Public Body - Breach of privacy | 66 |
| Request for Review – Privacy issues and complaints | 3 |
| Comments – Privacy Impact Assessment (PIA) | 6 |
| Comments – Health policies, Acts, processes | 2 |
| Miscellaneous and Administrative | 1 |



Access to Information and Protection of Privacy Act

Section 68 of the *ATIPPA* requires the Commissioner to provide an assessment of the effectiveness of the *Act* and to report on the activities of the office and any instances where recommendations of the Commissioner were not followed. In addition, I include some 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 2023/2024. Eight reports dealt with public bodies' applications for extensions of time to respond to access to information requests. Twelve reports reviewed public bodies' deemed refusals to respond to access to information requests. Three reports reviewed the sufficiency of public bodies' responses to access to information requests. Two reviewed privacy breach notifications provided by public bodies and two reviewed complaints that a public body had collected, used, or disclosed personal information without legal authorization.

All review reports are publicly available at <https://www.canlii.org/en/nt/ntipc/>.¹³

The Commissioner may issue orders at the conclusion of reviews dealing with access to information requests. These orders are binding on public bodies.¹⁴ To monitor compliance, orders will typically direct the public body to report back to our office on its performance under the order. Thus far there have been no appeals of any orders. However, there have been some instances where public bodies have failed to provide their responses within the time set by an

¹³ Past years' decisions are also available on-line on this free public database. With few exceptions, we do not publish reports on extension applications.

¹⁴ Per section 36 of the *ATIPPA*

order. As discussed above, this failure appears to be caused by the public body not dedicating sufficient resources to the task.

The Commissioner may make formal recommendations to a public body when dealing with privacy breaches.¹⁵ If a privacy breach is “material”¹⁶ 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 must decide whether to follow a recommendation and must report to the Commissioner regarding the implementation of any accepted recommendations.

Time Extension Requests

Public bodies have 20 business days to respond to an access to information request, and they can extend this period once for up to 20 business days in certain circumstances.¹⁷ Any further extension requires authorization by the Commissioner. An application for authorization must be submitted prior to expiration of the existing time period. If the time period expires first, the *Act* deems this to be a refusal to respond.¹⁸

I issued two orders in 2023 that have not yet been complied with. These were instances of deemed refusal and the orders compelled the public body to provide the responses. In each case more than six months has elapsed¹⁹ since the order was made. The source of delay, I am advised, lies with the public body, not the APO. Such delay amounts to a failure to comply with a legally binding order.²⁰ Fortunately, this is unusual behaviour.

Time extensions for third-party consultation

My office received nine extension-of-time requests from public bodies and issued eight Review Reports. These extensions were required to allow public bodies time to consult with third parties. Consultation is necessary where third-party personal information may be disclosed in a response to an access to information request. Third-party consultation requires 55 business days to complete,²¹ which is only available if an extension is authorized by the Commissioner.

In the normal course where the public body requires a 55-business-day extension to conduct third-party consultation, there is no basis for the IPC to deny an authorization. The authorization process is essentially a ‘rubber stamp’. I restate last year’s recommendation:

¹⁵ Division E of Part 2 of *ATIPPA*

¹⁶ The *Act* does not define this term but there are factors to consider set out in subsection 49.9(2).

¹⁷ See section 11(1)(a)-(d)

¹⁸ See section 8(2) of the *Access to Information and Protection of Privacy Act*

¹⁹ As of June 14, 2024.

²⁰ Section 36 of the *Access to Information and Protection of Privacy Act* specifies that, subject to an appeal, the head of a public body shall comply with an order of the Information and Privacy Commissioner made under section 35. There was no appeal in either case.

²¹ This includes a 40-business-day period to render a decision and a 15-business-day appeal period.

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

Delay in Responding to Access Requests – Resourcing the APO

The Access and Privacy Office (APO) provides support to all GNWT departments²² to fulfill their ATIPPA obligations. This approach can serve the public well, bringing together essential knowledge and experience, and creating efficiency in the access to information process.

In last year’s annual report, I noted an increase in deemed refusal²³ complaints despite there being a decrease in requests for time extensions. My office continues to receive requests for review of deemed refusals; in some instances, responses have been several months overdue.

The Act provides a process for extending the time to respond. A public body may extend the time once for up to 20 business days. Any further extension requires application to my office for an order. Public bodies can only apply for an extension *before* the existing time period expires. Failure to provide the response or to seek an extension in the time allowed amounts to a deemed decision to refuse to provide a response.

A decision to not use the process provided by the statute suggests either a lack of capacity to follow that process or a disregard for the Act’s procedural requirements. As the timelines in the Act are clear, inadvertence is not a reasonable explanation for missing a deadline.

I am reasonably certain that delays are not intentional; delay is caused by the staffing being insufficient to meet the workload. It is difficult to understand why the Legislative Assembly created legal obligations for public bodies without ensuring public bodies had the capacity to discharge those obligations. This is an ongoing source of concern for my office and frustration for members of the public who seek access to government records on a timely basis.

Previously, the government has 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.”²⁴ It is fair to say that the resources available to the APO do not provide sufficient capacity to meet the workload.

The 2024/2025 GNWT budget approved funding for two positions in the APO “to help meet its responsibilities to the public under the *Access to Information and Protection of Privacy Act*.” To place this in context, two positions at the APO were approved in 2019, to last until 2024. The

²² And the Northwest Territories Housing Corporation.

²³ If a public body does not provide its response to an access request within the time allowed by the Act, then this is deemed to be a decision to refuse to provide a response, pursuant to section 8(2).

²⁴ 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

practical effect is that the positions are not “new” but simply continue the existing staffing level rather than reducing it as originally budgeted. Since then, despite requests for increased resources, and despite evidence that public bodies’ legal obligations are not being met due to lack of resources, no new resources have been provided to assist the APO.

The APO is housed within the Department of Justice. If the Minister of Justice intends to respond to access to information requests in a timely manner, then something needs to change.

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

Reviews of Draft Legislation

Pursuant to section 67(1)(c) of the ATIPPA, the Information and Privacy Commissioner may provide comments on the implications for privacy protection arising from proposed legislation. We did not receive any draft legislation for review this fiscal year.

We did receive requests to review other materials. In April 2023, the Department of Health and Social Services provided for comment a draft of an agreement being developed between the department and an indigenous organization regarding the provision of child welfare services. The document was an early draft, and we provided some general comments and questions. It is encouraging to see privacy concerns being addressed at early stages in the development of such documents.

| Annual Comparison of ATIPPA Files | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 |
|--|------------------|------------------|------------------|------------------|
| Review - Access to records & reviewing redactions to records | 26 | 17 | 4 | 10 |
| Review - Fees, delays, Ext. 's by APO, process, deemed refusal | 8 | 18 | 8 | 25 |
| Review - 3rd party requests | 4 | 9 | 1 | 0 |
| Comments - Acts, legislation, bills, speeches, policies | 8 | 6 | 3 | 3 |
| Comments - PIA's | 0 | 0 | 1 | 0 |
| Privacy Issues - Breach notifications & complaints | 26 | 31 | 19 | 11 |
| Extension of Time - Requests from Public Bodies to OIPC | 0 | 13 | 19 | 9 |
| Corrections - To personal information | 1 | 0 | 1 | 1 |
| FPT Commissioners - Working groups & legislation | 1 | 0 | 0 | 0 |
| Misc. - Admin. files, office matters, OIPC initiated | 1 | 0 | 1 | 3 |
| Request from Public Body to Disregard ATIPP request | 0 | 1 | 0 | 0 |
| Total Files | 75 | 95 | 57 | 62 |

Health Information Act

Review Reports

My office received 66 reports of privacy breaches from health information custodians this year. I issued five review reports under the *Health Information Act*. These reports, like those issued under the *Access to Information and Protection of Privacy Act*, are available at <https://www.canlii.org/en/nt/ntipc/>.

Subparagraph 173(b) of the *Health Information Act* requires the Commissioner to report on recommendations that were made in a report to a health information custodian that were not accepted. Recommendations in four review reports were accepted; as discussed below, there was one report where a recommendation was only partially accepted.

Alternative Resolutions

Privacy breaches will be addressed through a formal review when an individual requests a review or if the Commissioner determines it is warranted.²⁵ Another approach is to work with the health information custodian and an individual using an alternate dispute resolution process²⁶ or, where appropriate, by providing comment and guidance and identifying relevant resources for consideration. Informal processes have led custodians to develop measures to prevent privacy breaches and to respond better to breaches when they occur. Formal reviews are not the only method for resolving a privacy breach and helping a custodian to prevent similar future events. Where appropriate, my office will continue to employ such alternative approaches to resolving privacy breaches.

Responding to Commissioner's Recommendations

At the conclusion of a review the Commissioner issues a report that 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.²⁷ The *Act* deems a failure to notify the Commissioner of the decision within 30 days as a decision *not* to follow the Commissioner's recommendations.

If a recommendation is accepted, the custodian must 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*

²⁵ On request by an individual under Section 134 or on the Commissioner's own initiative under section 137.

²⁶ As contemplated under section 138.

²⁷ Section 156.

section 49.14 creates just such an obligation.²⁸It would be helpful to have a mandatory reporting process on the implementation of recommendations.

Recommendation 3: *The Department of Health and Social Services should consider implementing a policy, or the Legislative Assembly should consider amending the Health Information Act, to require health information custodians to report to the Commissioner regarding the implementation of accepted recommendations.*

A Recommendation Not Accepted

The *Health Information Act* requires the Commissioner to identify any recommendations made in a review that are not accepted by a health information custodian. This occurred once this year.²⁹ In a review of an unauthorized disclosure of personal health information caused by faulty software, I made two recommendations respecting the Department of Health and Social Services' use of Privacy Impact Assessments (PIAs). The PIA assessing the software in question noted the possibility of a privacy breach caused by the very type of error that occurred. The PIA did not arrive in my office until months after the software had been implemented and long after the privacy breach had occurred. I recommended that the Department should complete PIAs during the planning phase of a project and that it should amend the *Privacy Impact Assessment Policy* to expressly require PIAs to be completed during the development of a project and to be submitted to the Information and Privacy Commissioner with a reasonable time for comment.

The Department did not accept the recommendations, stating that it already prepares PIAs during the planning phase and pointing out that section 175 of the *Health Information Act* does not specify a timeline for submitting a PIA or for the Commissioner to provide comment. The Department noted that the legislative review of the *Health Information Act*³⁰ will begin in early 2024 and our comments will be reviewed again in that process.

It may be appropriate to adopt legislative provisions for PIAs similar to section 42.1 of the *Access to Information and Protection of Privacy Act*.³¹ PIAs are a planning tool intended to design privacy protection into information and communication systems; they are not intended as an end-of-project evaluation tool. That said, there is no reason why the Privacy Impact Assessment Policy could not be amended to address this concern.

²⁸49.14. 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.

²⁹ *Re Department of Health & Social Services*, 2023 NTIPC 37 <https://canlii.ca/t/k1tw2> (CanLII)

³⁰ Per section 195.1, the *Health Information Act* is to be reviewed every 10 years. The Act came into force in 2015.

³¹ This section was added in 2019 and came into force July 30, 2021.

Incidence of Privacy Breaches

The number of new *Health Information Act* files decreased from 120 last year to 78 this year, and the number of privacy breach notifications from health information custodians decreased from 105 to 66. This is a significant improvement!

The following custodians reported breaches this year:

- Northwest Territories Health and Social Services Authority (NTHSSA)
- Department of Health and Social Services (DHSS)
- Hay River Health and Social Services Authority (HRHSSA)
- Tłıchq Community Services Agency (TCSA)
- Ring's Pharmacy in Hay River

| Breach Notifications by Health Custodian | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 |
|---|------------------|------------------|------------------|------------------|
| NTHSSA | 55 | 134 | 99 | 48 |
| DHSS | 1 | 63 | 5 | 7 |
| HRHSSA | 3 | 5 | 1 | 2 |
| TCSA | 7 | 4 | 0 | 8 |
| Ring's Pharmacy in Hay River | 0 | 0 | 0 | 1 |
| Total Files | 66 | 206 | 105 | 66 |

The Northwest Territories Health and Social Services Authority (NTHSSA) submitted the majority of the breach notices. This is to be expected as the NTHSSA provides health services to most communities in the Northwest Territories. It is encouraging that the number of new breach notices for both NTHSSA and the Department has decreased to the level of four years ago. The COVID-19 pandemic undoubtedly contributed to the surge in privacy breaches. It is difficult to predict the longer-term trend.

Privacy breaches continue to occur while faxing personal health information, when sending emails, printing documents, and using electronic health information systems. We are seeing an increasing number of incidents associated with scanning of printed reports into electronic format and then linking these to individuals' electronic medical records: sometimes the wrong report goes on the wrong person's medical record. A common cause of many of these errors is momentary inattention to detail. Whether an employee is sending a fax, sending an email, or linking a lab report to a patient's electronic medical record, getting the details correct is critical, both to protect patient privacy and to ensure patients' medical care is never compromised by information mismanagement.

It follows that the employees must be provided the appropriate training and support to ensure that they know what to do.

Recurring Issues in Privacy Breaches

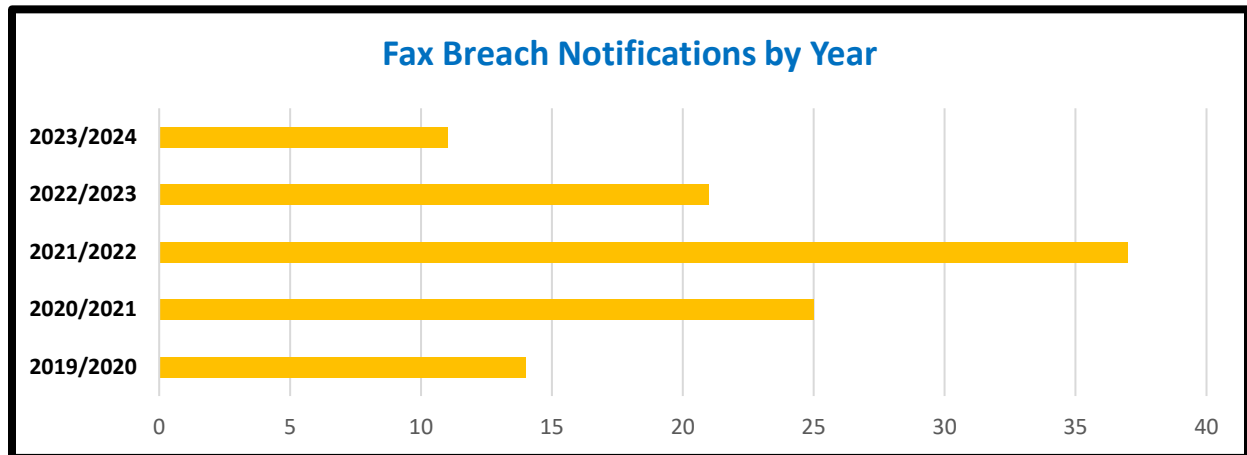
Faxing

There were 11 privacy breach notifications involving faxing errors (23% of NTHSSA’s breach notices) this fiscal year. Privacy breaches with the use of fax machines have been addressed in past review reports and Annual Reports.³² Faxing has also been the subject of comment by the Standing Committee on Government Operations.³³ The chart below suggests that improvements have been effective.

The GNWT has previously advised it intends to reduce the use of faxing related to provision of health and social services. In 2022, the NTHSSA created a system-wide policy to govern faxing of patient information. The policy states “only information which is urgent for the continuity of patient care should be transmitted by fax.” This is a useful restriction; however, the same restriction appears in the predecessor policy document from 2011.³⁴

The OIPC will continue to monitor this issue.

Recommendation 4: *Health information custodians should continue to reduce or eliminate the use of fax machines to transmit personal health information.*



Email

We continue to see privacy breaches when personal health information is emailed to the wrong email address, or to the wrong email group. Sometimes the wrong documents are attached to an email. Again, momentary inattention to detail is a common underlying factor.

³² 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>

³³ 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

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

Applying passwords to documents or using Secure File Transfer (SFT) can reduce the possibility of an unintended recipient being able to access someone else's personal information. Emails sent to groups should use the "bcc" function. These security measures are already specified to some degree in the GNWT's *Electronically Stored and Transferred Information Policy*. Comprehensive privacy training is also essential: employees need to be aware of the relevant privacy-protective measures they can use and of the applicable privacy policies that should guide their actions.

Recommendation 5: *Health information custodians should use secure electronic transmission measures when transmitting personal health information. Privacy training for employees should include detailed instruction on the use of secure electronic transmission measures.*

Privacy Training

Creating and maintaining a strong culture of privacy awareness and sensitivity to privacy issues is essential to prevent privacy breaches. Training in privacy protective policies and procedures is essential to creating a privacy-protective workplace culture, helping to avoid incidents that proceed from momentary inattention when handling personal health information. Employees working with personal health information need to keep privacy top of mind, and this requires express support from management and regular reinforcement through training.

The Department of Health and Social Services (DHSS) created its *Mandatory Training Policy* in 2017, which requires 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 prevent privacy breaches and to respond appropriately in the event of a breach.

Employees acting in positions without appropriate privacy training, and management inadequately documenting training, continue to be issues. Custodians will often address training deficiencies as part of their response to breach events, but this should not be necessary if custodians comply with the *Mandatory Training Policy*. Adequate employee training requires dedicated resources and on-going support from leadership and management.

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.*

Delay in Breach Notification

We continue to receive notices of privacy breaches several months after the custodian became aware of the incident; sometimes it can be several months more before a final report is received. The HIA requires notice to be provided as soon as reasonably possible.³⁵ Individuals should receive timely notice: they have the primary interest in protecting their own privacy.

The *Privacy Breach Policy* that guides NTHSSA and other health information custodians differs slightly from the legislation on this question of notice. It only requires notice after a full investigation has confirmed a privacy breach occurred. This is not, in my view, an appropriate policy direction as it is inconsistent with the statutory requirement for notice to be given as soon as reasonably possible. Notice should be given as soon as a privacy breach has been confirmed; there is no need to wait for the outcome of a full investigation. A full investigation will be needed to determine all the relevant details of a privacy breach, but this will typically proceed after the custodian learns that a breach occurred.

Providing notice allows an individual whose privacy has been breached to ask questions, make decisions, or take some action. There is no interest served in withholding notice until after a full investigation, and it does not accord with the legislative requirement to give notice as soon as reasonably possible.

Recommendation 7: *The Health and Social Services Privacy Breach Policy should be amended to require notice to be given to the affected individual(s) and to the Information and Privacy Commissioner as soon as reasonably possible once a privacy breach has been confirmed.*

Recommendation 8: *The Legislative Assembly should consider amending section 87 of the Health Information Act to require a health information custodian to give notice of a privacy breach within a specific time period.*

Privacy Impact Assessments

Our office reviewed and commented on six Privacy Impact Assessments (PIAs) this year. Five were submitted by the Department of Health and Social Services, regarding projects involving wastewater testing, expansion of the 811 health advice line, a new public health data repository, adopting an on-line mental wellness monitoring technology, and an archiving and communication system for electronic images and reports. Hay River Health and Social Services Authority submitted a PIA regarding the BDM Pharmacy Information system which replaced its then-existing pharmacy information system that had become obsolete.

³⁵ Section 87

Under the *HIA*, a PIA is used to identify potential privacy risks posed by new health care information or communication systems, or changes to existing systems.³⁶ The Act allows the Commissioner to comment on a PIA,³⁷ ostensibly so the health information custodian can consider those comments when finalizing design and implementation plans. Completing a PIA early in a project’s planning phase accords with the ‘privacy by design’ principle. Ideally, a PIA should be completed and provided for review and comment at an early stage of project development so that any comments from the Commissioner can be considered and incorporated where appropriate.³⁸ For comparison, the *ATIPPA* now stipulates these requirements for PIAs.³⁹

We are seeing improvement. For instance, the PIA addressing expansion of the 811 Health Line Service demonstrated that recommendations from the PIA review of the original 811 service had been considered. Our common goal is effective protection of patient privacy.

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

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

| Annual Comparison of HIA Files | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 |
|--|-----------|------------|------------|-----------|
| Breach Notification | 66 | 206 | 105 | 66 |
| Health Privacy Complaints | 10 | 4 | 2 | 3 |
| Comments on Privacy Impact Assessments | 7 | 15 | 9 | 6 |
| Comments on Health Policies, Acts, etc. | 3 | 8 | 1 | 2 |
| Corrections to Personal Health Information | 0 | 0 | 0 | 0 |
| Misc. - Admin. Files, office matters, OIPC initiated | 1 | 0 | 1 | 1 |
| Special - OIPC initiated projects | 0 | 1 | 2 | 0 |
| Total Files | 87 | 234 | 120 | 78 |

³⁶ Section 89

³⁷ Section 175

³⁸ 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

³⁹ See section 42.1 of ATIPPA



Interjurisdictional Activity

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

The annual FPT Information and Privacy Commissioners' conference was held in Quebec City in September 2023. In addition to receiving jurisdictional reports and several presentations on emerging issues, the conference finalized two resolutions: one addressing the need to protect the interests of young people in regard to privacy protection and access to information,⁴⁰ the other addressing the protection of privacy of employees in the workplace.⁴¹ Each resolution contains background references, making them helpful to those seeking to better understand the context of these issues.

In November 2023 our Assistant Commissioner and our Investigator participated in the annual Investigators' Conference. This learning event took place online and by all accounts it was a beneficial experience. Our office will be attending again this year.

⁴⁰ [Putting best interests of young people at the forefront of privacy and access to personal information - Office of the Privacy Commissioner of Canada](#)

⁴¹ [Protecting Employee Privacy in the Modern Workplace - Office of the Privacy Commissioner of Canada](#)

Final Thoughts

The possibility of bringing community governments under the governance of the *Access to Information and Protection of Privacy Act* has been developing for well over a decade. We still are not quite there.

In 2014, the Department of Municipal and Community Affairs (MACA) distributed a paper titled “*Possible Application of the ATIPP Act to Community Governments.*” MACA distributed the paper widely and sought feedback. In 2015 MACA published a “*What we heard*” document regarding the issue, acknowledging that the Information and Privacy Commissioner (my predecessor) had recommended the government “make every effort to bring municipalities under existing territorial access to information and protection of privacy legislation.”

In 2019, amendments were made to the *ATIPPA* to allow municipal governments to be designated as public bodies under the Act. Designation as a public body is made by regulation. The amendments came into force July 30, 2021, but as yet no such regulation exists. This means two things: the public still has no legal right of access to records held by community governments, and any protection of personal information derives from the *Personal Information Protection and Electronic Documents Act*.⁴² That protection governs only personal information of community governments’ employees, not personal information the community government holds about residents or others. This situation has existed since before the *ATIPPA* came into force in 1996.

The right to privacy has a constitutional ‘home’ in section 8 of the *Canadian Charter of Rights and Freedoms*. Many of the territorial government’s records contain personal information about us, and that personal information is protected by rules in the governing legislation: the *Access to Information and Protection of Privacy Act* and the *Health Information Act*. Our ability to access information under the *ATIPPA* has been characterized as quasi-constitutional, and it is without question fundamental to a responsible democratic government: citizens can hold their government responsible only insofar as they can know what their government is doing.

The debate about whether community governments should be subject to the *ATIPPA* has long been concluded in the affirmative. What remains is for the territorial government to take the necessary steps to prepare community governments to be able to comply with the Act, and then to pass the appropriate regulation. The need for resources to accomplish this goal was identified years ago. There is, again, no debate that designating community governments as public bodies under the Act is an important and well-established public policy goal. The government needs to get on with the work of making this happen, before yet another decade passes.

⁴² PIPEDA is federal legislation that applies to private organizations engaged in commercial activity and to personal information of employees of federal works, undertakings or businesses.

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. (Pg 12)*

Recommendation 2: *Public bodies should review their legal obligations to respond to access to information requests and evaluate their capacity to provide responses within the legislated time periods. They should also ensure, either collectively or individually, that the APO is appropriately resourced so that it can assist public bodies to respond reliably to access to information requests within the legal time periods and to comply with the relevant procedural requirements. (Pg 13)*

Recommendation 3: *The Department of Health and Social Services should consider implementing a policy, or the Legislative Assembly should consider amending the Health Information Act, to require health information custodians to report to the Commissioner regarding the implementation of accepted recommendations. (Pg 15)*

Recommendation 4: *Health information custodians should continue to reduce or eliminate the use of fax machines to transmit personal health information. (Pg 17)*

Recommendation 5: *Health information custodians should use secure electronic transmission measures when transmitting personal health information. Privacy training for employees should include detailed instruction on the use of secure electronic transmission measures. (Pg 18)*

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. (Pg 18)*

Recommendation 7: *The Health and Social Services Privacy Breach Policy should be amended to require notice to be given to the affected individual(s) and to the Information and Privacy Commissioner as soon as reasonably possible once a privacy breach has been confirmed. (Pg 19)*

Recommendation 8: *The Legislative Assembly should consider amending section 87 of the Health Information Act to require a health information custodian to give notice of a privacy breach within a specific time period. (Pg 19)*

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

Recommendation 10: *The Legislative Assembly should consider amending section 89 of the Health Information Act to include similar provisions regarding privacy impact assessments as mandated in section 42.1 of the ATIPPA. (Pg 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 location is suite 703 in the Northwest Tower
5201 – 50th Avenue, Yellowknife, NT**