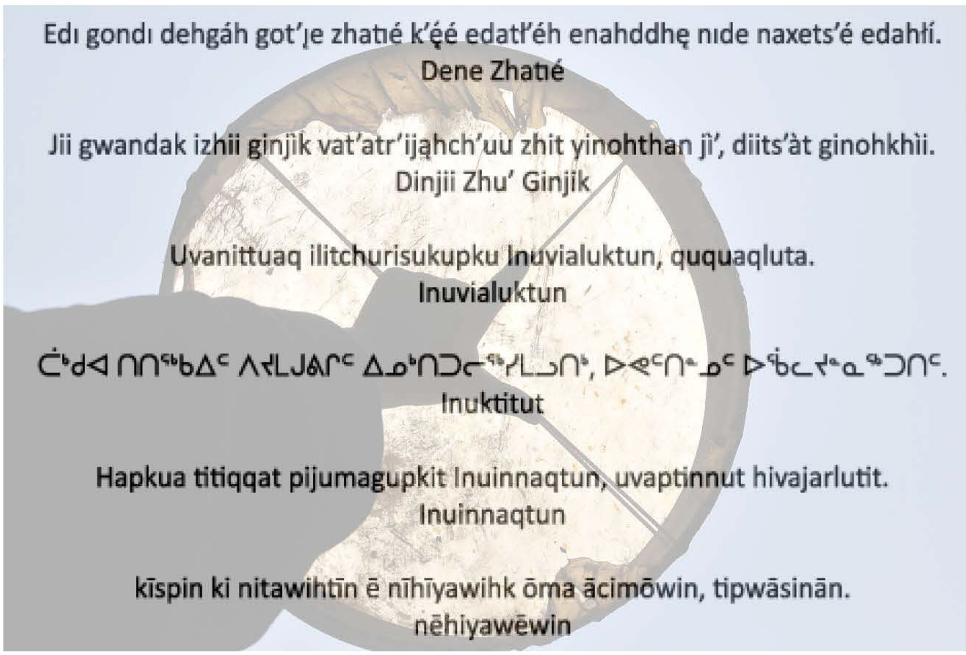
OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

Northwest Territories

Annual Report
2025 - 2026

K’áhshó got’ı̨ne xədə k’é hederı ɂedı̨htl’é yerınıwę nı dé dúle.
Dene Kədə́

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



Edı gondı dehgáh got’ı̨e zhatıé k’ę́ę́ edatł’éh enahddhę nıde naxets’é edahłí.
Dene Zhatıé

Jii gwandak izhii ginjìk vat’atr’ijąhch’uu zhit yinohthan jì’, diits’àt ginohkhìi.
Dinjii Zhu’ Ginjìk

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.
Inuvialuktun

ᑖᒃᑯᐊ ᑎᑎᖅᑲᐃᑦ ᐱᔪᒪᒍᕕᑦ ᐃᓄᒃᑎᑐᓕᕐᓯᒪᓗᑎᒃ, ᐅᕙᑦᑎᓐᓄᑦ ᐅᖄᓚᔪᓐᓇᖅᑐᑎᑦ.
Inuktitut

Hapkua titiqqat pijumagupkit Inuinnaqtun, uvaptinnut hivajarlutit.
Inuinnaqtun

kīspin ki nitawihtīn ē nīhīyawihk ōma ācimōwin, tipwāsinān.
nēhiyawēwin

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

Office of the Information and 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, 2026

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, 2025, to March 31, 2026.

Yours 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

I am pleased to provide this annual report on the activities of the Office of the Information and Privacy Commissioner (OIPC). 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* (ATIPPA) and section 173 of the *Health Information Act* (HIA).

Access to information and protection of privacy are fundamental to a functional democracy. People need to be able to find out what their government is doing on their behalf; governments must protect individuals' personal information.

With some exceptions, we find public bodies are generally aware of their obligations under the *Access to Information and Protection of Privacy Act*, but they often struggle to manage their records and respond to requests for access to information within the statute's time limits.

The Department of Justice has an Access and Privacy Office (APO) that supports all government departments and Housing NWT to respond to access to information requests, but it is overwhelmed with work: between September 2025 and May 2026, 68 percent of access to information requests received a late response. The office has never had enough staff to handle the number of requests it receives, and the requests are increasingly large and complex. When a request involves records that have been poorly managed, the amount of work required to conduct a diligent search can increase dramatically. A response delivered late is a failure by a public body to discharge its legal obligations.

The Legislative Assembly approved a supplementary appropriation for the Access and Privacy Office in May of 2026. We are cautiously optimistic this will lead to improvement and will be monitoring the situation.

We note that public bodies are improving their capacity to identify and respond to privacy issues. For example, the Department of Health and Social Services (DHSS) conducts monthly audits of the electronic medical record (EMR) system to identify potentially unauthorized access events. The auditing process cannot identify all possible instances of unauthorized access, but nonetheless it is proving effective: the number of instances of unauthorized access reported to my office has increased since the DHSS began this auditing process in 2022.

Of course, the purpose of an auditing program is not merely to detect unauthorized access, but to deter the behaviour. As employees realize their access is logged and audited, and that there are personal consequences for such behaviour, I expect the number of incidents to decrease.

The government completed administrative reviews of both the *Health Information Act* and the *Access to Information and Protection of Privacy Act* in 2025-26. My office provided submissions to both of those review processes. I look forward to reviewing any changes to the statutes as and when the legislature may choose to consider them.

Last, I was reappointed in November of 2025. I am honoured to serve for a second term.

Financial Report

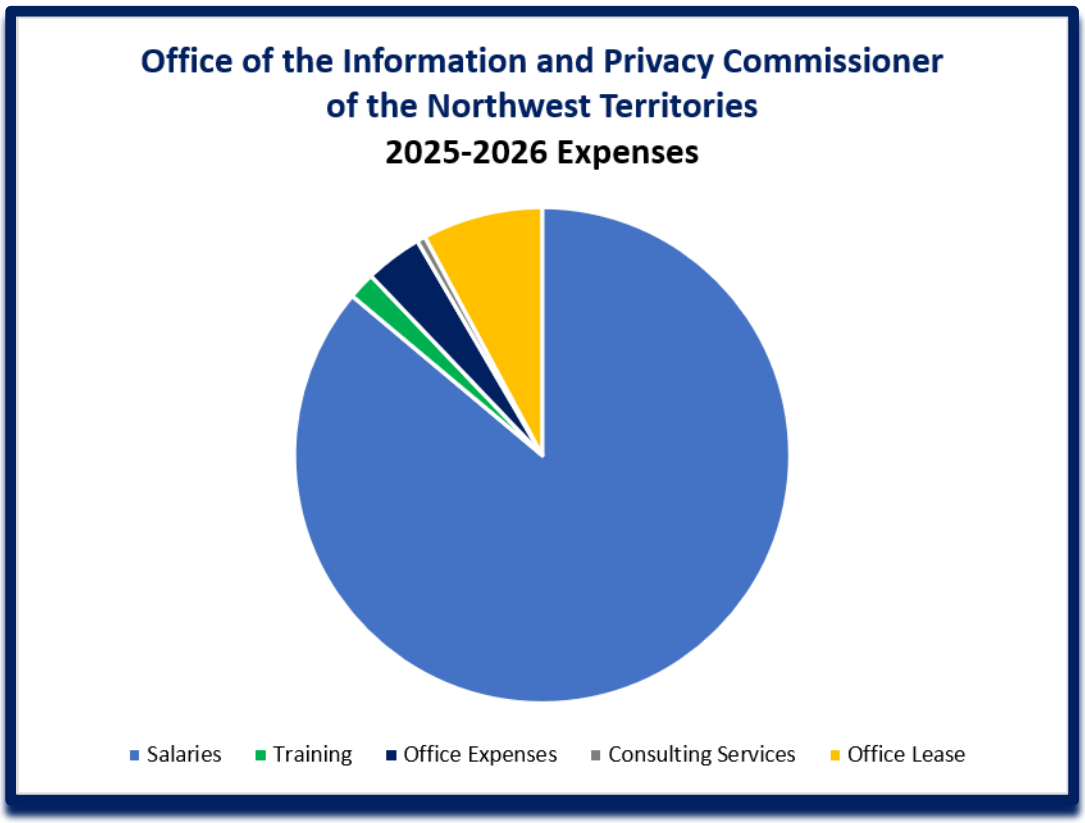
The approved budget for the Office of the Information and Privacy Commissioner (OIPC) of the Northwest Territories for the fiscal year 2025-2026 was $963,000.00. Salaries and office expenses amounted to $957,328.84, and $5,671.60 was returned to the Legislative Assembly. A detailed breakdown is outlined in the charts on the next page.

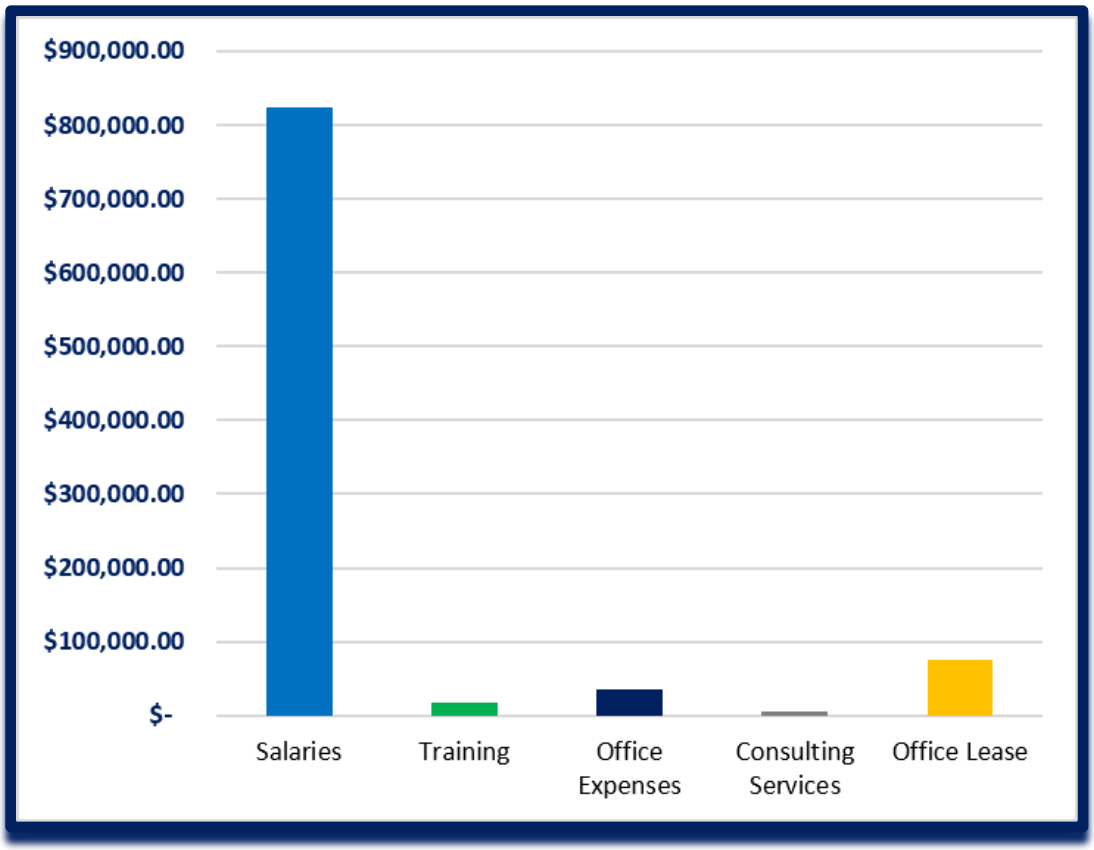
The administration of the OIPC budget was uneventful. There was an increase in salary expense due to yearly increases as per the collective agreement and the retro-active pay after the conclusion of the appeal for the salary assessment for the Early Resolution Officer job description.

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
2024-2025	$922,907.23	4
2025-2026	$957,328.84	4

Professional development and training are a continuing expense. Online courses and in-person conferences support our staff to learn and apply best practices and to stay abreast of developments in privacy and access to information practices.

We continue to retain a consultant to assist with reviewing Privacy Impact Assessments (PIAs). The need fluctuates with the number of assessments submitted to my office.


Office of the Information and Privacy Commissioner
of the Northwest Territories
2025-2026 Expenses
Salaries
Training
Office Expenses
Consulting Services
Office Lease


$900,000.00
$800,000.00
$700,000.00
$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 Lease

The Year in Review

The Office of the Information and Privacy Commissioner opened 140 files between April 1, 2025, and March 31, 2026. This reflects a marked decrease in the number of privacy breach reports involving personal health information. As explained below, this is due primarily to the Northwest Territories Health and Social Services Authority (NTHSSA) adjusting its reporting threshold in 2025.

Overview of the Activity

Access to Information and Protection of Privacy Act (ATIPPA)

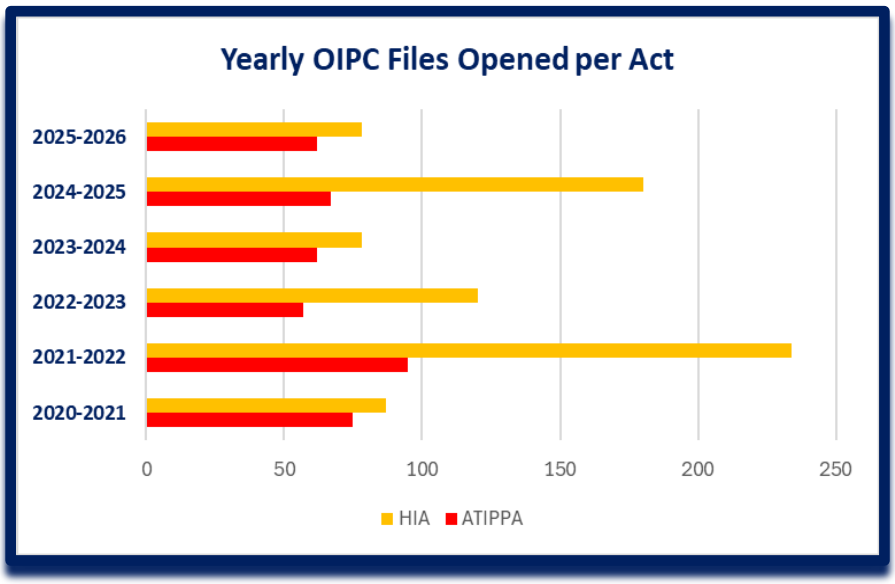
The OIPC opened **62 files** under the *Access to Information and Protection of Privacy Act*.

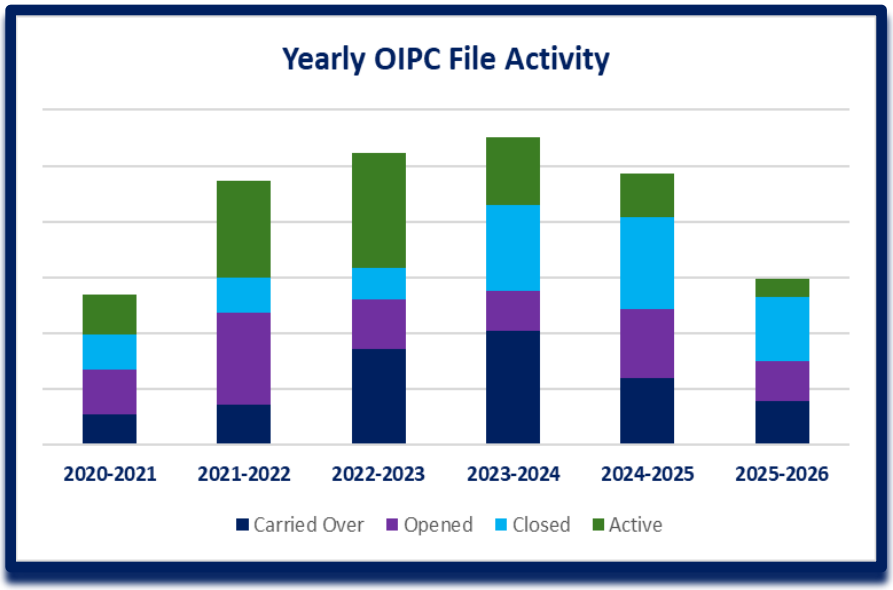
Requests for Review – Challenging redactions made in access response	10
Requests for Review – Fees, delays, process or refused access	17
Requests for Review – Breach of privacy complaint	4
Requests for Review – Third-party request	6
Requests for time extension to respond to access request	16
Notifications from public body - Breach of privacy	5
Consultations/Comments – Acts, Bills, PIAs, Policies	2
Miscellaneous, Administrative & OIPC Initiated	2

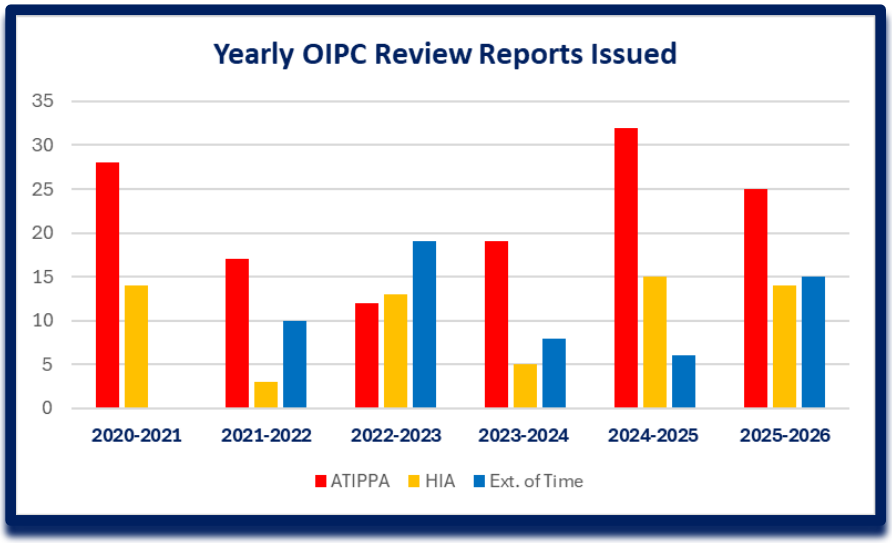
Health Information Act (HIA)

The OIPC opened **78 files** under the *Health Information Act*.

Notifications from public body - Breach of privacy	65
Requests for Review – Privacy issues and complaints	6
Comments – Privacy Impact Assessment (PIA)	6
Comments – Health policies, Acts, processes	0
Miscellaneous and Administrative	1


Yearly OIPC Files Opened per Act
2025-2026
2024-2025
2023-2024
2022-2023
2021-2022
2020-2021
0
50
100
150
200
250
HIA
ATIPPA


Yearly OIPC File Activity
2020-2021
2021-2022
2022-2023
2023-2024
2024-2025
2025-2026
Carried Over
Opened
Closed
Active


Yearly OIPC Review Reports Issued
35
30
25
20
15
10
5
0
2020-2021
2021-2022
2022-2023
2023-2024
2024-2025
2025-2026
ATIPPA
HIA
Ext. of Time

Reviews and comments on draft legislation

Pursuant to section 67(c) of the ATIPPA, the Information and Privacy Commissioner may provide comments on the implications for privacy protection arising from proposed legislation. Late in 2025-26, I was invited to comment on a few provisions being considered for the proposed *Safer Communities and Neighbourhoods Act*. Bill 49 was introduced during the Spring 2026 sitting of the Legislative Assembly.

Both the HIA and ATIPPA were subject to review in 2025-26. I provided written comments in both reviews and encouraged the responsible departments to propose improvements to the legislation. The government has indicated it is not considering amendments to either Act for the remainder of the 20th Assembly. However, should the Legislative Assembly consider amending either the HIA or the ATIPPA, our office will be pleased to provide further input.

Mandatory privacy training

Diligent attention to security can prevent unauthorized access to confidential information. It can also reduce the demand on time and resources required to respond effectively to such events. Most importantly, good security protects privacy, and training helps to keep security a priority.

In July 2025, a person entered an office building over the lunch hour while staff were away.[1] The person walked through two unlocked doors, looked through paperwork that had been left unsecured on a desk, and stole cheques that were being held for pickup. This theft was only possible because several security measures failed. The incident was over in five minutes, but responding to the breach and mitigating its effects took months.

[1] https://www.canlii.org/en/nt/ntipc/doc/2026/2026ntipc132/2026ntipc132.html

In a case from 2025-26, the Department of Health and Social Services' privacy audit discovered that a clinic assistant working for the Northwest Territories Health and Social Services Authority (NTHSSA) had been inappropriately accessing their own and other clients' medical charts in the electronic medical record system (EMR).[2] At the time, EMR audit reports were delayed by approximately nine months, meaning that by the time the health authority realized there was an issue, the behaviour had been ongoing for nine months. NTHSSA privacy staff met with the employee to discuss the audit from their first month on the job and required them to re-take privacy training. This appears to have stopped the employee's misuse of the EMR system: training can be effective!

Pursuant to the Department of Health and Social Services' Mandatory Training Policy,[3] employees of DHSS and the three health authorities are required to take privacy training each year. For existing employees, annual training provides an opportunity to refresh their familiarity with their legal obligations and to consider anew how to incorporate privacy protection into their everyday workflows. New employees require training to ensure they are aware of their obligations and are aware of the various privacy-protective policies, procedures, and tools that are available in the workplace.

***Recommendation:* Public bodies should continue to ensure all employees receive annual privacy training appropriate to their position.**

[2] https://www.canlii.org/en/nt/ntipc/doc/2026/2026ntipc128/2026ntipc128.html
[3] Referred to in Ministerial Directive MD 2023-04

Section 68 of the ATIPPA directs me to provide an assessment of the effectiveness of the act and to report on the activities of my office and any instances where my recommendations were not followed.

Annual Comparison of ATIPPA Files	2020-2021	2021-2022	2022-2023	2023-2024	2024-2025	2025-2026
Review - Access to records & reviewing redactions to records	26	17	4	10	10	10
Review - Fees, delays, process, deemed refusals	8	18	8	25	27	17
Review - 3rd party requests	4	9	1	0	1	6
Comments - Acts, legislation, bills, speeches, policies	8	6	3	3	3	2
Comments - PIA's	0	0	1	0	1	0
Privacy Issues - Breach notifications & complaints	26	31	19	11	13	9
Extension of Time - Requests from Public Bodies to OIPC	0	13	19	9	11	16
Corrections - To personal information	1	0	1	1	0	0
FPT Commissioners - Working groups & legislation	1	0	0	0	0	0
Misc. - Admin. files, office matters, OIPC initiated	1	0	1	3	1	2
Request from Public Body to Disregard ATIPP request	0	1	0	0	0	0
Total Files	**75**	**95**	**57**	**62**	**67**	**62**

Review reports

My office issued 25 review reports under the ATIPPA in 2025-2026. Review reports are available at https://www.canlii.org/en/nt/ntipc/.[4]

A review of a public body's response to an access to information request may result in an order that is binding on the public body. When appropriate, an order will direct the public body to report on its performance of the order. This assists our office to monitor compliance. At times, a public body has failed to comply with an order within the time allowed. Frequently, the explanation is a lack of resources within the public body, or within the Access and Privacy Office, or sometimes both.

When dealing with privacy breaches, a public body must report a privacy breach to the Commissioner if it is "material." If the privacy breach creates a "real risk of significant harm" to one or more individuals, the Commissioner may recommend the public body take additional 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 then decide whether to follow a recommendation and must provide a report to the Information and Privacy Commissioner on the status of its implementation of accepted recommendations.

[4] Past years' decisions are also available on this free public database. With a few exceptions, we do not publish reports on time extension applications.

Technology is changing records management and privacy protection

Technology is having an ever-increasing effect on information and privacy. Public bodies rely on computerized systems to manage their records, and most communication involves technology to some extent. This brings new benefits and risks; public bodies are adapting to rapid change while trying to minimize negative effects.

When the *Access to Information and Protection of Privacy Act* came into force in 1996, many records were still created on a typewriter and filed in hard copy. Today, a record may be a piece of paper, but it is much more commonly in electronic format, whether as a document, a photograph, an email, a text message, or a "chat" on an on-line meeting platform such as MS Teams or Zoom. Public bodies are struggling with records management. The proliferation of email and the ease of creating electronic records have dramatically increased the number of records public bodies must manage.

A challenge associated with the widespread use of electronic communication systems is the effective and secure management of electronic records. Some government departments employ the Digital Integrated Information Management System (DIIMS) to manage and store electronic records; others do not. A significant proportion of electronic records are transitory messages with no business value and do not need to be retained. But many do need to be retained and must be managed according to the applicable retention schedule, such as the Operational or Administrative Records Classification Systems (ORCS and ARCS). The focus is always on the content of the record, not the format or the computer program used to create it. Employees need training and support to ensure records are created and managed correctly and are available when needed, such as for responding to an access to information request.

<u>Recommendation:</u> Government departments should ensure their business practices and records management practices are aligned with the applicable retention schedules and should ensure their employees are trained to implement those practices.

Training and resources for education bodies

In recent years it has become apparent that education councils struggle to meet their legal obligations when they receive a request for access to information. These public bodies collect and use highly sensitive personal information, much of it relating to children but also parents and staff. Through reviewing responses to requests for information, we discovered that education council employees often have not received training regarding what the ATIPPA requires.

While conducting a review involving an education council, we learned that the public body stored its records somewhat haphazardly; its employees used personal devices and personal email accounts to conduct work.[5] To help it respond to an access to information request, it ultimately hired a law firm. In another case involving a different education council, an applicant contacted my office after receiving no response to an access to information request. My staff contacted the head of the public body and learned that no search for responsive records had begun and there was no intention to respond to the access request.[6]

The public's right of access to records applies to all public bodies, including the education councils and education authorities created under the *Education Act*. Records must be created and managed so that they are available for a variety of purposes, including responding to access to information requests. Trained staff and appropriate records management systems are essential to meeting a public body's obligations, including education bodies.

<u>Recommendation:</u> The Department of Education, Culture and Employment should support education councils and education authorities to develop capacity to discharge their obligations under the ATIPPA.

[5] https://www.canlii.org/en/nt/ntipc/doc/2025/2025ntipc106/2025ntipc106.html
[6] The applicant eventually withdrew their request for review, so no report was published.

Information management in workplace investigations

In 2025-26 my office opened several files relating to matters in which a public body had collected personal information from individuals who believed their information would never be disclosed to specific people. Most of these files related to workplace investigations and involved witnesses who provided information to investigators about workplace conduct of others. These witnesses believed their evidence would never be disclosed to the subject of the investigation. This caused real concern when the subject of the investigation requested access to the material created or gathered for the purpose of the workplace investigation.

Information created or gathered for a workplace investigation is governed by section 24.2 of the ATIPPA. This section was part of the 2019 amendments and came into force in 2021. The amendment addresses a very specific category of record, and places very precise controls on its disclosure. This is appropriate given the highly sensitive nature of such information, including personal information of witnesses.

Section 24.2 is only one of the exceptions to the public right of access to records. Other exceptions may still apply even if section 24.2 directs the public body to disclose; applying the various exceptions in the act can be complicated.

It is incumbent on the public body doing labour relations investigations to ensure witnesses in investigations are informed about how the information they provide will be managed; witnesses should not be surprised by the way the employer collects, uses, or discloses the information they provide, including their own personal information.

<u>Recommendation:</u> Public bodies conducting workplace investigations into labour relations matters should ensure that witnesses are aware that information they provide will be subject to the ATIPPA, including potential disclosure under section 24.2.

Local housing organizations

Many NWT residents live in public housing operated by local housing organizations (LHOs). LHOs are either local housing authorities created by ministerial order under the *Northwest Territories Housing Act,* or local housing associations created under the *Societies Act.*

LHOs are not public bodies listed in the *Access to Information and Protection of Privacy Regulations*, and thus not subject to the ATIPPA. However, in a practical sense, LHO records are subject to the public's right of access under Part 1 of the Act because LHO records are available to Housing NWT, which is a public body subject to the ATIPPA. Part 2 of the ATIPPA, which governs the collection, use, disclosure, and disposal of personal information, does not apply to LHOs.

LHO records contain personal information about their tenants – information for which tenants have a reasonable expectation of privacy. During 2025-26 I received a complaint about the way an LHO had used and disclosed a client's personal information. Responding to my inquiry, Housing NWT provided a copy of the confidentiality policy that LHOs are required to follow. The policy states that LHOs are subject to the ATIPPA. Later, however, Housing NWT declined to opine on the question of whether territorial or federal legislation – ATIPPA or PIPEDA[7] – governs LHOs' collection, use, and disclosure of personal information. It became apparent during the review that the LHO did not have a clear sense to which privacy protection legislation it is subject.

If LHOs are operating under the assumption that they are subject to the ATIPPA, it would be appropriate to formalize that status. It does not serve the public interest for LHOs to be uncertain about what privacy protection legislation applies to them.

<u>Recommendation:</u> The Executive Council should consider adding local housing organizations to the list of public bodies in Schedule A of the Access to Information and Protection of Privacy Regulations.

[7] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5

Annual Comparison of HIA Files	2020-2021	2021-2022	2022-2023	2023-2024	2024-2025	2025-2026
Breach Notification	66	206	105	66	173	65
Health Privacy Complaints	10	4	2	3	2	6
Comments on Privacy Impact Assessments	7	15	9	6	3	6
Comments on Health Policies, Acts, etc.	3	8	1	2	1	0
Corrections to Personal Health Information	0	0	0	0	0	0
Misc. - Admin. Files, office matters, OIPC initiated	1	0	1	1	1	1
Special - OIPC initiated projects	0	1	2	0	0	0
Total Files	**87**	**234**	**120**	**78**	**180**	**78**

Review reports

My office received 65 reports of privacy breaches from health information custodians this year. I issued 14 review reports under the *Health Information Act* (HIA). These reports are available at https://www.canlii.org/en/nt/ntipc/.

Subparagraph 173(b) of the HIA requires the Commissioner to report on any recommendations that were made in a report to a health information custodian that were not accepted. I am pleased to report that all recommendations were accepted.

Alternative resolution

My office resolves most privacy breaches without issuing formal review reports. Following receipt of a notice of a breach from the health information custodian, and later a final investigation report, we will assess the scope of the breach, evaluate any mitigations that were applied to avoid or minimize harm, and evaluate any measures taken to prevent similar breaches. Often the health information custodian will have addressed the cause(s) of the breach, and no further action will be necessary. Frequently, we will ask for additional information. We may provide comment and suggest measures to avoid similar breaches in the future, and we may identify relevant resources for consideration. Typically, this informal mode of resolution is used if there are no factual issues to resolve and the likelihood of significant harm is low. Informal processes typically conclude faster than a formal review.

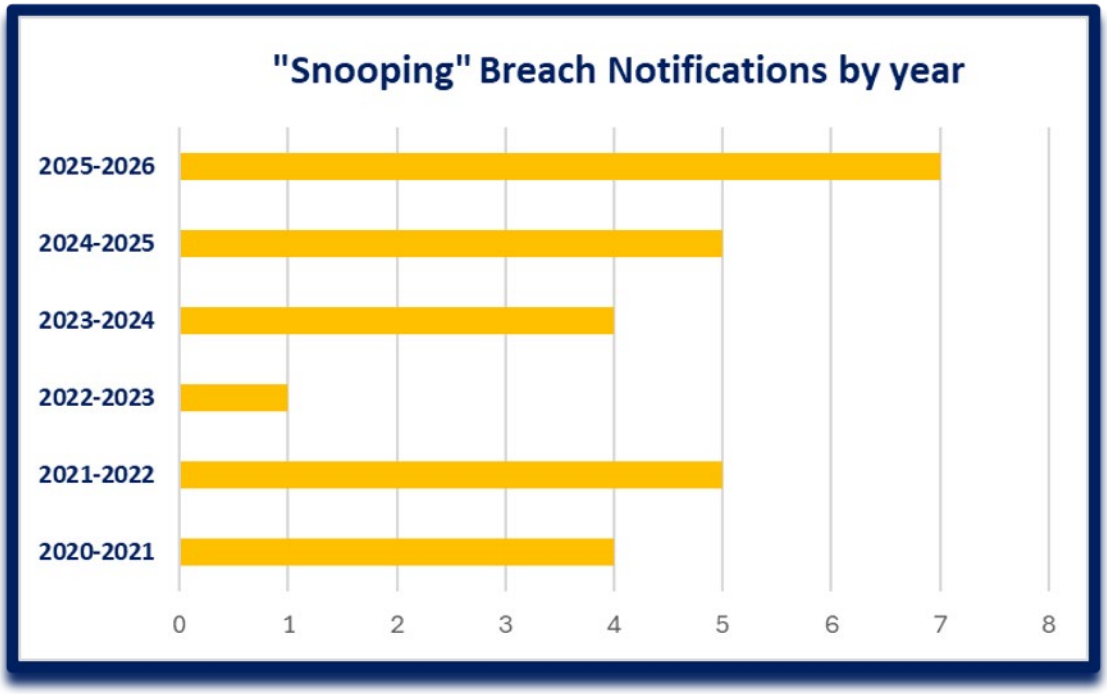
Implementing recommendations in a review report

A privacy breach review will often conclude with formal recommendations to the health information custodian, which then has 30 days to decide whether it will follow the recommendations. The HIA deems a failure to notify the Commissioner of the decision within 30 days as a decision to not follow the recommendations.[8] If a recommendation is accepted, the custodian must comply with the recommendation within 45 days.

[8] Section 156.

As noted in last year's annual report, the *Health Information Act* does not require reporting on the implementation of an accepted recommendation. In comparison, the ATIPPA section 49.14 creates just such an obligation.[9] It would be helpful to have a statutory reporting process on the implementation of recommendations.

Recommendation: ***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 on the steps taken to implement accepted recommendations.***



Identifying unauthorized access to personal health information

Most privacy breaches in the health system are inadvertent, momentary, and pose little risk to patients. Some, however, are deliberate, intentional violations of an individual's personal privacy. These can harm client trust in the health system, both for the affected individual and others. This is never acceptable.

The Department of Health and Social Services (DHSS) has assigned staff and resources to investigate misuse of the electronic medical record system. The DHSS and the health authorities conduct regular audits to identify possible unauthorized access to patient records.[10]

[9] 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.

[10] Sometimes referred to as "snooping".

This year's report shows an increase in the number of intentional privacy breaches. The cases reported to my office include a lab assistant who checked their own child's test results, a clinic assistant who accessed about two dozen patient charts without a legal reason, and a temporary employee who viewed 372 clients' records. The audit processes that the DHSS and the health authorities have developed over the last three years are producing results; health authorities are taking disciplinary measures when unauthorized access is discovered. As employees realize they will be discovered and disciplined for such behaviour, the number of these cases may be expected to drop.

Audit process

The example described on page 7 of this report (involving the clinic assistant)[11] demonstrates the need for properly resourced, timely audit processes. Delayed monthly audit reports continued to arrive at the health authority, showing the employee had been accessing charts nine months earlier. The employee eventually resigned. Had the behaviour been identified earlier, the subsequent privacy breaches may have been prevented.

There is currently a delay of six to nine months between an EMR access and the DHSS employee review of the audit to determine if there are any questionable access events. After DHSS reviews the audit report, it is sent to the head offices of the health authorities, who then send it to the employees (typically managers) tasked with investigating possible privacy breaches. This can also be a source of delay as these employees typically have additional responsibilities. The employees tasked with investigating privacy breaches are not located in the privacy unit at NTHSSA. Perhaps they should be.

<u>Recommendation:</u> DHSS and the health authorities should be directed to dedicate sufficient and appropriate resources to the EMR auditing function to ensure audits are completed on a timely basis.

[11] https://www.canlii.org/en/nt/ntipc/doc/2026/2026ntipc128/2026ntipc128.html

Challenges facing the NWT Health and Social Services Authority

Delays in completing reports concerning privacy breaches

Privacy breaches related to intentional staff misbehaviour are rare. When they do occur, the response often requires significant time and effort from staff and management. Some cases are one-time errors caused by a misunderstanding; others involve repeated, sometimes malicious misuse of client information. The latter behaviour can lead to significant disciplinary measures.

Intentional privacy breaches often require significant effort to investigate and typically involve a separate labour relations process. This can lead to significant delay in notifying the affected individuals and in completing the final privacy breach report.

Delay can seriously frustrate the efforts of affected individuals to mitigate their own harms. When notified promptly, they are in a better position to decide how to respond. Delay can render mitigation impossible.

Delays multiply the difficulties for health information custodians. Evidence can be lost if not collected soon after a breach; memories fade and witnesses can be difficult to locate months or years later.

One review in 2025-26 dealt with highly sensitive child and family services records found inside a binder that had been left unsecured in a rental unit used by visiting NTHSSA employees.[12] Upon discovery NTHSSA immediately secured the records, but then the investigation stalled. Key witnesses were not interviewed, and investigators took no steps to determine who had placed the records into the binder, or why. Someone placed the records into the binder, but who and for what purpose remains unknown. NTHSSA does not know because it did not ask at the time of discovery and did not investigate for many months following. More than a year passed after discovery before NTHSSA notified the affected individuals. A timely investigation might have identified what happened, the underlying causes, and preventative measures.

[12] https://www.canlii.org/en/nt/ntipc/doc/2025/2025ntipc122/2025ntipc122.html

NTHSSA has a privacy unit staffed with trained privacy specialists. Nevertheless, NTHSSA delegates much of the privacy breach investigation work to unit managers who may have little training in investigating privacy breaches and little time to devote to the task: they have health-care management responsibilities that sometimes take operational precedence. This frequently results in delayed or incomplete investigations.

<u>Recommendation:</u> The Legislative Assembly should encourage public bodies to develop a cohort of trained employees to investigate privacy breaches. Ideally, investigators should not be part of the operational hierarchy of the unit where the privacy breach occurs. The Legislative Assembly should ensure that public bodies have the resources necessary to properly conduct privacy breach investigations.

Changes to the reporting threshold - breach notifications from NTHSSA

As the chart below displays, the number of reported privacy breaches has decreased significantly this year. This is due to a change in NTHSSA's reporting policy threshold.

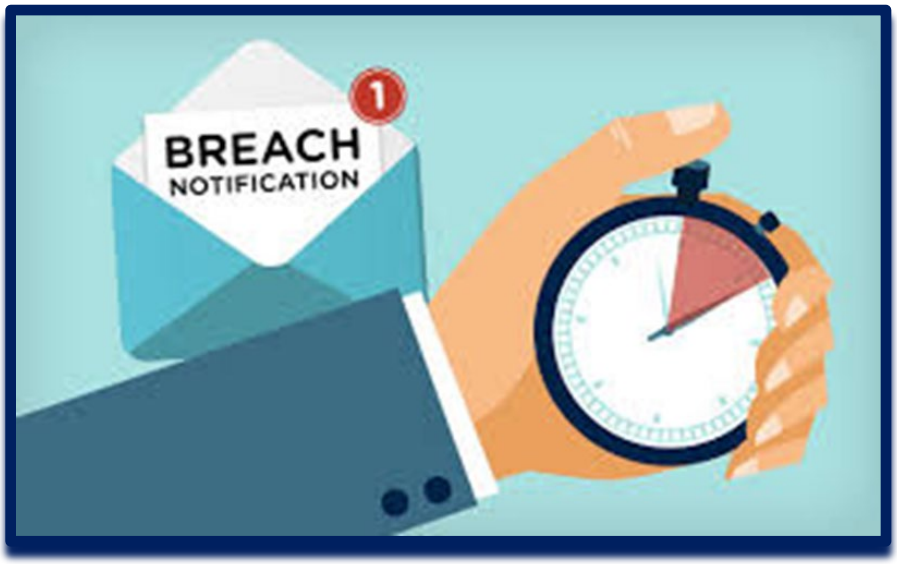
Breach Notifications by Health Custodian	2020-2021	2021-2022	2022-2023	2023-2024	2024-2025	2025-2026
NTHSSA	55	134	99	48	149	53
DHSS	1	63	5	7	6	6
HRHSSA	3	5	1	2	9	1
TCSA	7	4	0	8	9	5
Ring's Pharmacy in Hay River	0	0	0	1	0	0
Total Files	**66**	**206**	**105**	**66**	**173**	**65**

For the first 10 years the *Health Information Act* was in force,[13] NTHSSA notified the Commissioner of all privacy breaches, without consideration of the risk of harm to affected individuals. For example, in the 2024-25 fiscal year NTHSSA reported about 100 "scan/link" errors that arose when administrative staff misfiled documents in patients' electronic medical records (EMR), sometimes misdirecting them to incorrect care providers. These errors were often discovered within hours or days and fixed without delay. Personal health information was not disclosed outside the EMR, there were no delays in providing care, and the error did not affect clinical decisions. Technically, these instances of unauthorized use and disclosure of personal health information were privacy breaches; however, they typically did not pose any reasonable risk of harm to the affected individual.

Under the HIA, the health information custodian must investigate all privacy breaches and must notify all affected individuals. However, notice to my office is required only if the breach poses a reasonable risk of harm to the affected individuals.[14]

[13] The *Health Information Act* came into force in 2015.
[14] Per section 15(2) of the *Health Information Regulations*

Halfway through 2025-26, NTHSSA updated its reporting threshold to align more strictly with the requirements of the Health Information Regulations. The statistics for this year reflect this update: I received far fewer breach notifications from NTHSSA in 2025-26. As a result, statistics regarding the number of privacy breaches reported to my office cannot be compared directly to prior years as they reflect different reporting thresholds. Of course, NTHSSA remains responsible for investigating and notifying affected individuals of all privacy breaches; there is no threshold for notice to affected individuals.



Form of notice to affected individuals

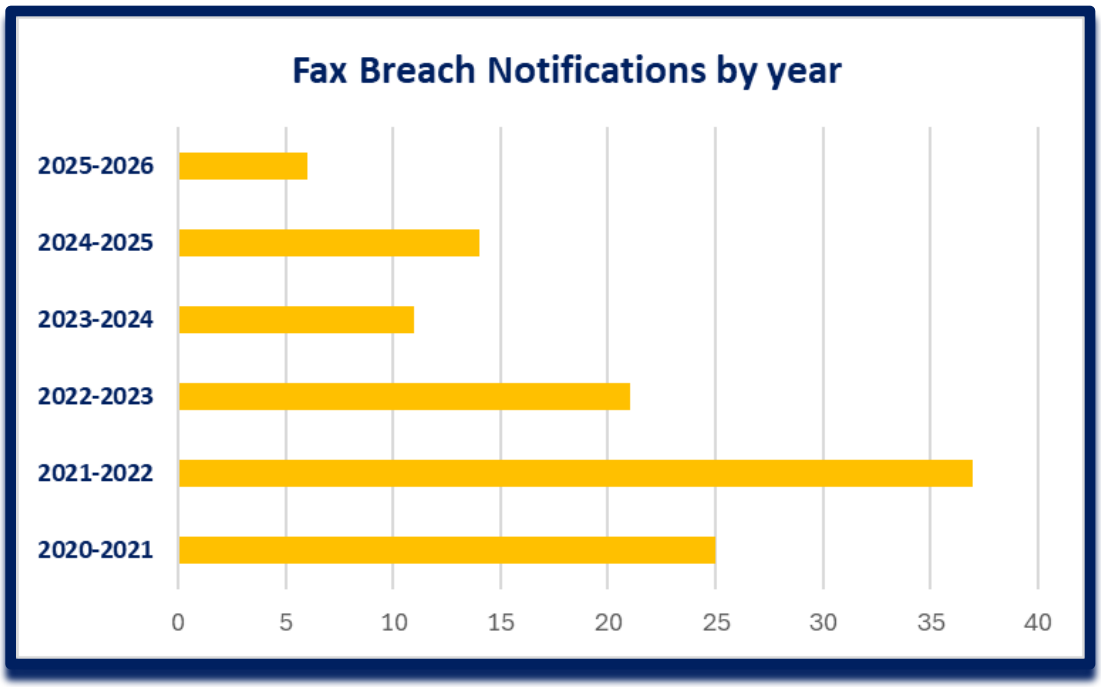
In 2025-26, my office received numerous emails and calls from people who had received notices of privacy breaches from the Northwest Territories Health and Social Services Authority. The notices typically contain an alert of a privacy breach but provide few if any details about what happened or what information was at stake. This generally leaves affected individuals uninformed and thus confused about the circumstances of the privacy breach. They are, as a result, unsure about the level of concern they should have and what steps, if any, they should take to protect their interests. Frequently, they became concerned with 'worst case scenarios,' worrying that their medical history had been deliberately accessed by unethical employees. This concern appears to arise when the notice provides insufficient information to understand even the basic nature of the breach. The reaction may be somewhat alarmist, but it is nevertheless understandable.

Notices that lack detail may nominally discharge a duty to give notice, but they do not usefully inform individuals of their situation or help them determine an appropriate response. Health information custodians should give affected individuals effective privacy breach notices. Notices should include the available relevant information about how a breach occurred, what information was misdirected, and what is being done to mitigate any harms. This should, in my view, increase public confidence that breaches are taken seriously and addressed.

Recurring issues in privacy breaches

Faxing

Fax machines have been a significant factor in privacy breaches since the HIA came into effect. These errors are typically caused by inattention, sometimes combined with a lack of familiarity with fax machines. NTHSSA's current policy directs staff to avoid using the fax except in urgent situations. As a result, when breaches occur there is typically an element of time sensitivity. This, of course, can make a breach even more problematic: sometimes when the information is needed most it is directed to the wrong place.



In response to ongoing concerns, NTHSSA's privacy staff has been encouraging the use of secure file transfer and EMR linking rather than faxing whenever possible. It appears that this has been effective: far fewer fax breaches are being reported to my office. We will continue to monitor this issue.

Privacy Impact Assessments

Our office reviewed and commented on Privacy Impact Assessments (PIAs) for

- An initiative to use the 811 service to respond to a TB outbreak for NTHSSA
- DHSS response to a TB outbreak for NWT residents
- NTHSSA, HRHSSA & TCSA - an initiative to use the 811 service for a smoking cessation program
- An upgrade to the Laboratory Information System for NTHSSA
- NTHSSA & DHSS Pneumatic Tube Delivery System
- Use of AI Scribe by NTHSSA & DHSS

Looking to the future, the Northwest Territories' electronic medical record system is aging, and the government is planning to replace it with a modern, integrated system for managing health records. This is a large project. The Department of Health and Social Services briefed my office on the project last year and we look forward to further engagement. At some point during the planning phase, we expect to receive a Privacy Impact Assessment for a proposed new system. We look forward to providing a thorough review of the project at that time.

Interjurisdictional Activity

The federal, provincial, and territorial Information and Privacy Commissioners meet online monthly to share information, hear presentations, and discuss policies, technology, legislative proposals, and various other topics and issues pertaining to access to information and protection of privacy. These regular meetings are a valuable forum to stay informed of policy developments at the national and international level.

Commissioners met in person in Alberta in October 2025. After the two-day conference, we issued joint resolutions on trust, transparency and democracy in an era of misinformation, and on protecting the privacy of children and youth through responsible use of educational technologies in the classroom.

My office routinely consults on matters where another Commissioner seeks an NWT perspective. Similarly, my federal, provincial and territorial counterparts have been invaluable resources.

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*[15] *(*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 ATIPPA.[16] With the amendments that came into force in 2021, municipalities may be designated as public bodies by regulation.[17]

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 ATIPPA 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 ATIPPA 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 ATIPPA that came into force in 2021 provided additional privacy breach response requirements and introduced privacy impact assessment requirements.[18]

The Commissioner provides independent review of public bodies' decisions and actions under both parts of the ATIPPA. 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, 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.

[15] *SNWT 1994, c 20.*
[16] Subject to limitations and exceptions set under ATIPPA or other legislation.
[17] No communities have yet been designated.
[18] Substantial amendments were passed in SNWT 2019 c.8 and came into force on July 30, 2021.

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 to access information and applying the relevant statutory exceptions can involve complex decisions. Independent oversight provides confidence that public bodies apply the ATIPPA correctly, helping to assure applicants that their rights are being upheld.

The *Health Information Act*

The *Health Information Act*[19] (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 Tłı̨chǫ 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 individuals[20] if personal health information is used or disclosed other than as permitted by the HIA, 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.[21] 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 HIA, or, in appropriate circumstances, the Commissioner may initiate a review independently. After conducting a review, the Commissioner will prepare a report and may make recommendations to the health information custodian. The health information custodian must notify the Commissioner of the health information custodian's decision to follow or not to follow the recommendation(s) 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.

[19] SNWT 2014, c 2.
[20] Section 87 of the *Health Information Act*.
[21] Section 87 of the *Health Information Act* and Section 15(2) of the *Health Information Regulations.*

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 review and comment on proposed legislation regarding possible implications for privacy protection or access to government information.

Summary of Recommendations

Recommendation 1: *Public bodies should continue to ensure all employees receive annual privacy training appropriate to their position. (Page 7)*

Recommendation 2: *Government departments should ensure their business practices and records management practices are aligned with the applicable retention schedules and should ensure their employees are trained to implement those practices. (Page 9)*

Recommendation 3: *The Department of Education, Culture and Employment should support education councils and education authorities to develop capacity to discharge their obligations under the ATIPPA. (Page 10)*

Recommendation 4: *Public bodies conducting workplace investigations into labour relations matters should ensure that witnesses are aware that information they provide will be subject to the ATIPPA, including potential disclosure under section 24.2. (Page 11)*

Recommendation 5: *The Executive Council should consider adding local housing organizations to the list of public bodies in Schedule A of the Access to Information and Protection of Privacy Regulations. (Page 12)*

Recommendation 6: *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 on the steps taken to implement accepted recommendations. (Page 14)*

Recommendation 7: *DHSS and the health authorities should be directed to dedicate sufficient and appropriate resources to the EMR auditing function to ensure audits are completed on a timely basis. (Page 15)*

Recommendation 8: *The Legislative Assembly should encourage public bodies to develop a cohort of trained employees to investigate privacy breaches. Ideally, investigators should not be part of the operational hierarchy of the unit where the privacy breach occurs. The Legislative Assembly should ensure that public bodies have the resources necessary to properly conduct privacy breach investigations. (Page 17)*

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

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)