Annual Report
2024 / 2025

Northwest Territories

OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
NORTHWEST TERRITORIES

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

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

Kīspin ki nitawihtīn ē nīhīyawihk ōma ācimōwin, tipwāsinān.
Cree

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

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

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

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

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

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.
Inuvialuktun

ᑖᒃᑯᐊ ᑎᑎᖅᑲᐃᑦ ᐱᓕᒍᔪᐱᒋᑦ ᐃᓄᒃᑎᑐᓕᖅᑭᓗᒃ, ᐅᕐᓂᑎᓐᓄᑦ ᓄᑦ ᐅᖅᑲᓕᕐᓐᓇᖅᑐᑎᑦ.
Inuktitut

Hapkua titiqqat pijumagupkit Inuinnaqtun, uvaptinnut hivajarlutit.
Inuinnaqtun

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

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

July 1, 2025

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, 2024, to March 31, 2025.

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 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*.

Privacy was in the news this year: several schools responded to a privacy breach at a software company; public offices dealt with thefts and break-ins; and health authorities sought effective ways to deter employee snooping. I issued reports about inappropriate disclosure of personal information during a procurement process, a counsellor who defaced a social worker's files left in an unsecured desk drawer, and a "reply all" error that disclosed a client's personal health information to over 200 people.

Northerners have been actively asserting their right to access records held by public bodies. My office dealt with numerous reviews of public bodies' responses to access requests for records involving the 2023 wildfires response, various procurement activities, and labour relations matters. Many of these have been complex and time-consuming. Public bodies frequently need more time to respond to these requests and sometimes miss the legislated deadlines.

I am encouraged by the government's interest in "open data" and other proactive disclosure initiatives. The Open Data repository should be a place where the public can go to obtain relevant information, both current and historical. This will require continuous upkeep by departments, and I strongly encourage them to devote resources to this activity.

Overall, the access and privacy system in the NWT continues to suffer from a lack of resources. The problem is at every level: some employees seem unaware that legislation applies to records they create, record management and security tools are available but underused, training is provided but not followed, privacy offices are understaffed, and leadership is not taking its

obligations seriously. Within health authorities, many privacy breaches are caused by employee inattention: staff are responding to urgent client needs within an understaffed system and do not take time to double-check their work. Errors contribute to a further drain on scarce resources when privacy breaches need to be investigated and responded to.

The experienced full-time staff at the GNWT's Access and Privacy Office are a significant benefit to public bodies. Their specialized skills allow them to respond professionally and with greater accuracy than less experienced staff, and their centralized role gives them a level of objectivity and independence that serves clients more effectively. This model is worth investing in; the increased capacity in the Access and Privacy Office will undoubtedly help government departments respond to access requests within the legislated timelines – something that continues to be a challenge.

Earlier this year the Access and Privacy Office advised my office that it is failing to provide responses within the time allowed under the statute about 60% of the time. This is an increase from 50% in 2022. We have seen a significant number of deemed refusal files, and in many of these instances the public body did not seek an extension of time to respond. This appears to be a product of insufficient staffing. I understand that two new indeterminate positions have been approved for the APO, which is encouraging.

NTHSSA's access to information and privacy unit has made steady progress in addressing breaches and responding to requests for access to information since it was established in 2022. I understand the privacy units in all of the health and social services authorities struggle to meet the requirements of the *Access to Information and Protection of Privacy Act* and the *Health Information Act*. Increased, dedicated resources for access to information and privacy protection would almost certainly help NTHSSA meet its legislated obligations.

Financial Report

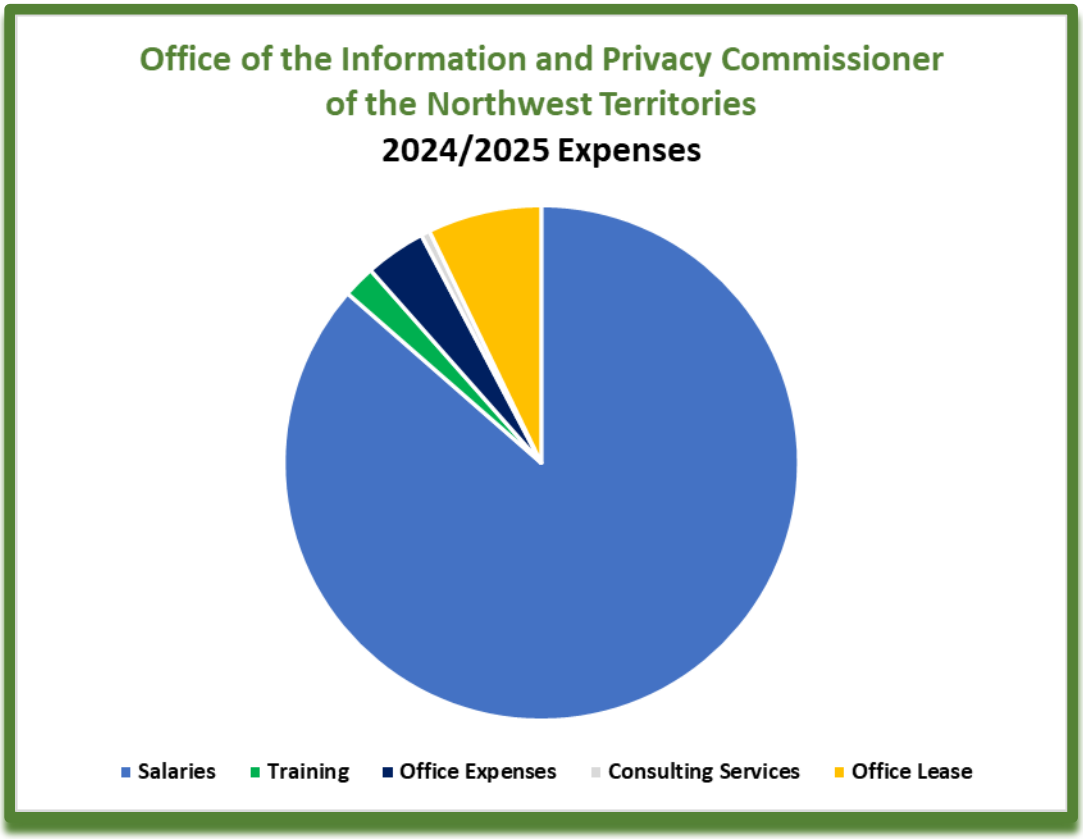
The approved budget for the Office of the Information and Privacy Commissioner (OIPC) of the Northwest Territories for the fiscal year 2024/2025 was $947,000.00. Salaries and office expenses amounted to $922,907.23, and $24,092.77 was returned to the Legislative Assembly. A detailed breakdown is outlined in the charts on the next page.

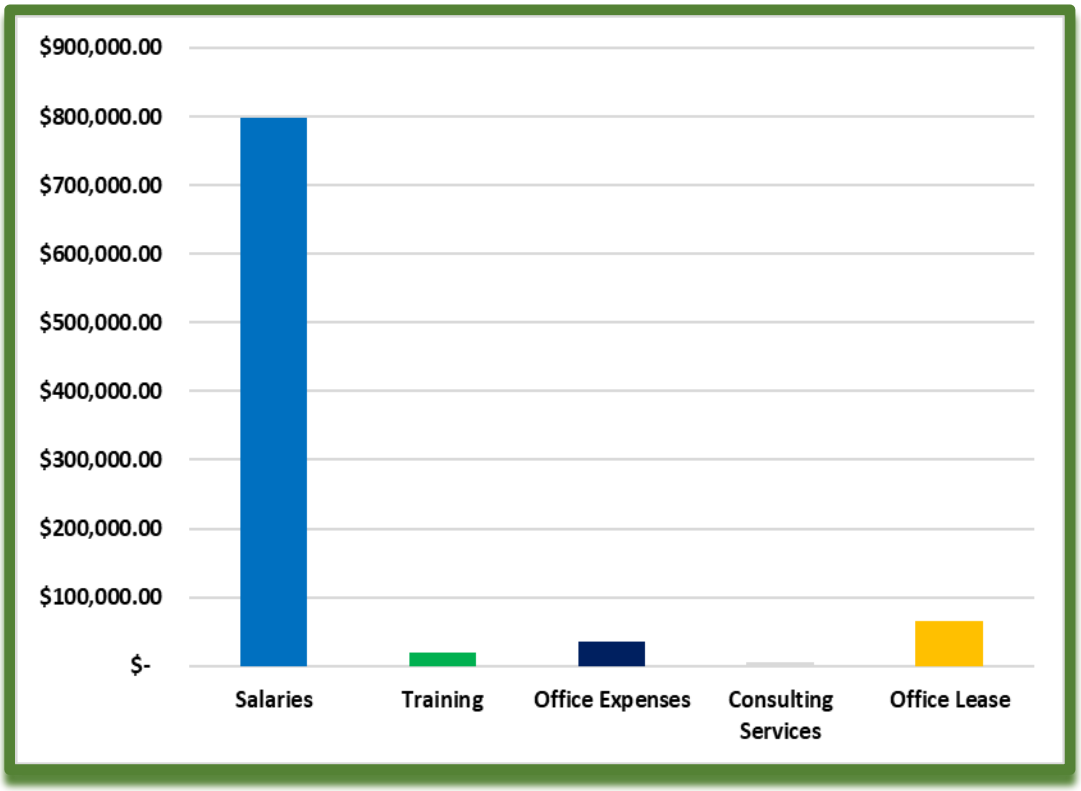
Generally speaking, the administration of the OIPC budget was uneventful. There was an increase in salary expense due to the retroactive pay from the signing of the collective agreement which increased the Compensation and Benefits by $66,644.00. We expect a separate increase this year following the review of the assessment for the Early Resolution Officer job description.

Professional development and training are a continuing expense. Online courses and in-person conferences support our staff to learn and apply Canadian 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. The need fluctuates and is correlated with the number of assessments submitted to my office.

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


Office of the Information and Privacy Commissioner
of the Northwest Territories
2024/2025 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 247 files between April 1, 2024, and March 31, 2025, a significant increase from the 140 new files opened the previous year, but less than the post-COVID high of 329 in 2021/2022.

Overview of the Numbers

Access to Information and Protection of Privacy Act (ATIPPA)

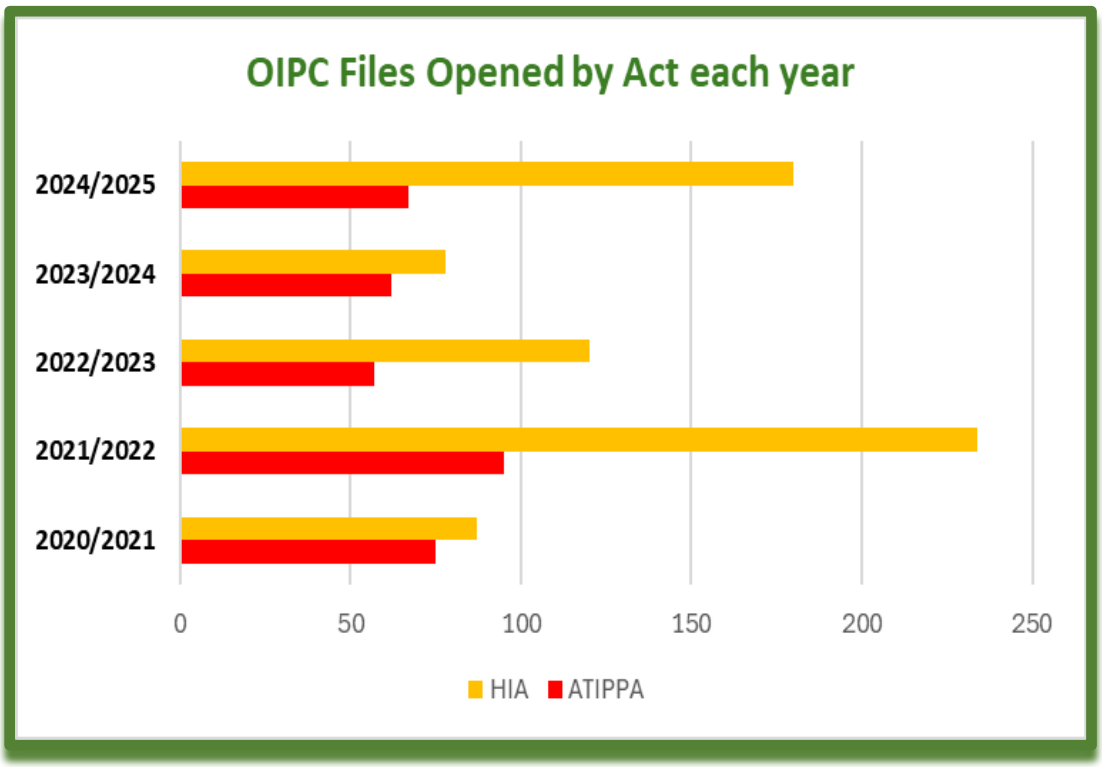
The OIPC opened **67 files** under the *Access to Information and Protection of Privacy Act*.

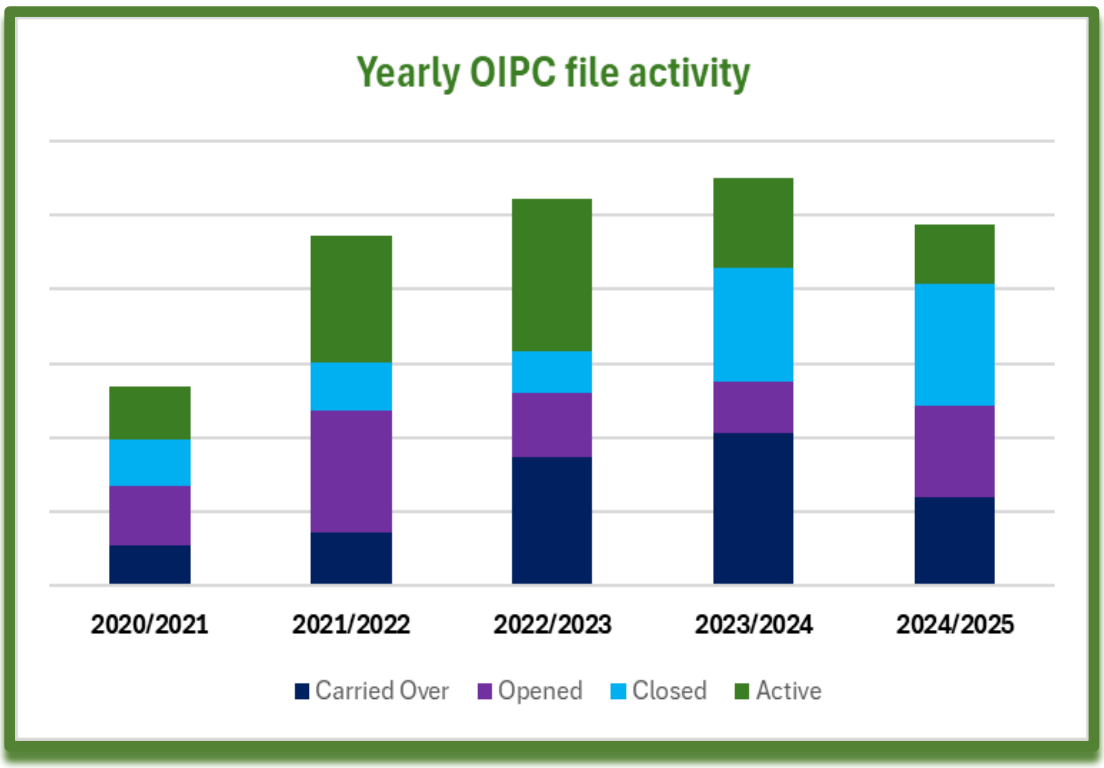
Requests for Review – Challenging redactions made in access response	10
Requests for Review – Fees, delays, process or refused access	27
Requests for Review – Breach of privacy complaint	4
Request for Review – Third-party request	1
Requests for time extension to respond to access request	11
Notifications from public body - Breach of privacy	9
Consultations/Comments – Acts, Bills, PIAs, Policies	4
Miscellaneous, Administrative & OIPC Initiated	1

Health Information Act (HIA)

The OIPC opened **180 files** under the *Health Information Act*.

Notifications from public body - Breach of privacy	173
Requests for Review – Privacy issues and complaints	2
Comments – Privacy Impact Assessment (PIA)	3
Comments – Health policies, Acts, processes	1
Miscellaneous and Administrative	1


OIPC Files Opened by Act each year
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
Carried Over
Opened
Closed
Active

Access to Information and Protection of Privacy Act

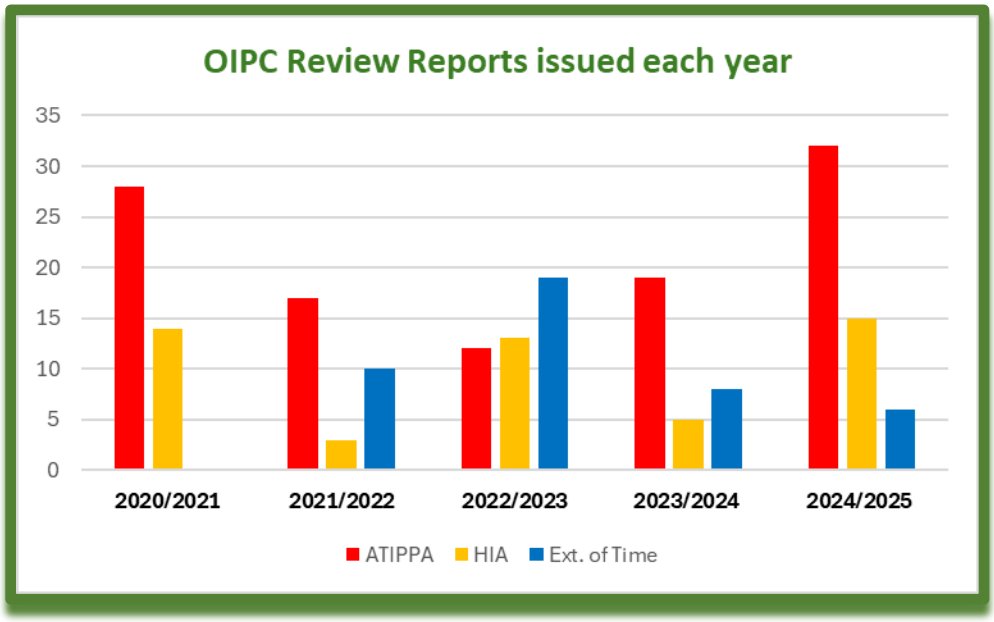
Section 68 of the *ATIPPA* requires me to provide an assessment of the effectiveness of the *Act* and to report on the activities of my office and any instances where my recommendations were not followed.

Review Reports

My office issued 32 review reports under the *ATIPPA* in 2024/2025. Current and past years' review reports are available at https://www.canlii.org/en/nt/ntipc/.[1]

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 report on its implementation.



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

Challenges in Responding to Requests

Public bodies must respond to access to information requests as mandated in the legislation. Some public bodies fail to do so: in one extreme case in 2024/2025, a public body waited two weeks before assigning staff to respond to a request, then tried to claim an extension far in excess of the legal limit, and then told the applicant he would need to pay for a professional to assist the public body to respond to his request. The public body also wholly refused to disclose certain records. This was all contrary to the requirements of the *Act*. It was readily apparent that the employee responding to the access request was completely unfamiliar with the work required to respond to an access request, or what the public body's legal obligations were. Even responding to questions from my office strained the public body's capacity.

The work involved in responding to an ATIPP request can be significant, and there is no substitute for knowledge and experience. A skilled ATIPP coordinator can help an applicant to better describe the desired records and thereby limit the work – and the time -- required to search for responsive records and prepare the response. During 2024/2025, my office received several requests to review public bodies' responses to requests for "all records" about some topic. Generally, a request for "all records" is overly broad and likely to greatly increase the volume of responsive records. This will typically increase the time and complexity involved in the response, only to provide records that are of little to no interest to the applicant.

A helpful solution for government departments has been the creation of the Access and Privacy Office, which provides the public with a single point of contact to submit access to information requests and provides public bodies with expert assistance in responding to access requests. Unfortunately, the Access and Privacy Office does not provide its full suite of services to all public bodies. Smaller public bodies are often challenged to respond to access requests according to the *Act*.

The implicit premise in the legislation is that public bodies will resource their access and privacy function to meet their legal obligations. Public bodies are explicitly required to make every reasonable effort to assist an applicant and to respond to an applicant openly, accurately, completely, and without delay.[2] Fulfilling these legal obligations requires resources dedicated to preparation – staff training, implementation of record management systems, etc. If a public body does not train its access to information coordinators, if it does not implement and use appropriate record management systems, and if it does not ensure all staff are aware of the rules governing public access to records, then even a minor access request can be problematic and cause a significant drain on the public body's resources.

The Access and Privacy Office has been under-resourced almost since inception. In early 2025 I was advised by the Access and Privacy Office that 60% of responses to access requests were delivered late, i.e., after the relevant time had expired. In 2022 the figure was 50%. Plainly, this is not a satisfactory service standard. I am aware that two staff positions have been added

[2] See section 7(1) of the Act.

recently to the APO, and this will undoubtedly have a positive effect. Whether this will be sufficient to enable public bodies to fulfill their obligations under the statute remains to be seen.

In my view, it would be helpful if the Access and Privacy Office was resourced to assist all public bodies subject to the *Act*. The Access and Privacy Office's expertise could help all public bodies fulfill their obligations to the public in less time and with less errors. Of course, that would likely require a further expansion of the Access and Privacy Office.

Delay in Responding to Access Requests – Resourcing the APO

The Access and Privacy Office (APO) provides support to all GNWT departments[3] to fulfill their *ATIPPA* obligations. This approach can serve the public well. It brings essential knowledge and experience together and creates efficiency in the process.

If a public body fails to provide its response to an access to information request within the time allowed, the failure is deemed to be a decision to refuse under section 8(2). In most cases, the public body has not actually decided to refuse to respond and maintains an intention to deliver the response.

The *Act* provides a process for extending the time to respond beyond the initial 20 business days. A public body may extend the time once for up to 20 business days. Any further extension requires authorization from the Commissioner. Public bodies can only apply for this *before* the existing time period expires.

There were nine applications for extensions this year. There were 27 requests for review by individuals who had not received responses from public bodies within the statutory periods. Of these, I issued 17 orders directing the public body to provide its response. In nine cases the public bodies provided their responses shortly after the request for review was filed, obviating the need to complete a review. In one case, the review proceeded to address the diligence of the public body's efforts to respond to the access request.

[3] And the Northwest Territories Housing Corporation.

Delay is an ongoing source of frustration for applicants, public bodies, the Access and Privacy Office, and my office. The Legislative Assembly has created legal obligations for public bodies without ensuring those public bodies have the capacity to meet those obligations. As mentioned above, the two new positions at the Access and Privacy Office should address the delay that is endemic in the access to information process. Whether it will be sufficient remains to be determined. My office will monitor the situation.

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.[4] Any further extension requires authorization by the Commissioner. An application for authorization must be submitted before the existing time period expires; otherwise, the *Act* deems this to be a refusal to respond.[5]

I authorized nine extensions this fiscal year. Two other requests were denied: one because the deadline to apply had already expired, the other because the grounds for the request were not sufficient. In six cases the public body failed to deliver the records within the extended period. In four of these, more than 100 business days elapsed after the extended period ended; in one other, the last set of records was delivered over one year after I authorized a 55 day extension. In one other, an extension was denied on October 21, 2024, and the response remains undelivered 8 months later.[6]

These six cases are a direct result of the lack of resources provided to the Access and Privacy Office. Public bodies are ultimately responsible for providing responses in the time allowed, but as a practical matter it is the Access and Privacy Office that shoulders much of the burden. I understand that in most cases, the Access and Privacy Office is the 'bottleneck' that slows down the response time.

Time extensions for third-party consultation

Consultation is necessary where third-party personal information may be disclosed in a response to an access to information request. It requires 55 business days to complete,[7] 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:

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.*

[4] See section 11(1)(a)-(d)
[5] See section 8(2) of the *Access to Information and Protection of Privacy Act*
[6] *Department of Environment and Climate Change (Re)*, 2024 NTIPC 71 (CanLII)
[7] This includes a 40-business-day period to render a decision and a 15-business-day appeal period.

Proactive Disclosure

Section 72 of the *Act* requires public bodies to establish and publish categories of records that do not contain personal information and that can be made available without a formal request for access. Section 71 requires public bodies to make certain types of manuals, instructions, guidelines, rules and policy statements available without a formal access request. Section 5.1 directs public bodies to disclose information where there is a risk of significant harm to the environment or to the health or safety of the public.

In short, there is a broad requirement for public bodies to publish information so that it is accessible to members of the public without going through the formal process. As most information is now created and stored electronically, this should not be an onerous task.

Some public bodies are more proactive in publishing information than others. In general, government departments' websites appear to be up to date; understandably, some smaller agencies' websites are less extensive, but some also appear to be missing current information. Section 71 and 72 may not be well understood by all public bodies, but given the efficiencies of making information easily available, and given their legal status, I strongly urge all public bodies to devote sufficient resources to fulfilling the requirements of these sections.

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.

In May 2024 the Department of Health and Social Services sought comment on proposed changes to the *Child and Family Services Act*. The changes relate to information sharing between the GNWT, federal government, and Indigenous governments in the context of child welfare. I provided some general comments and urged the Department to complete a privacy impact assessment and consult my office again when it has drafted the proposed amendments.

In late March 2025 the Department of Executive and Indigenous Affairs consulted regarding a draft information-sharing agreement involving service delivery through Government Services Officers. I provided some preliminary comments and questions about this integrated program and urged the Department to submit a privacy impact assessment for review as contemplated under section 42.1 of the *ATIPPA*.

The Department of Health and Social Services is conducting a 10 year statutory review of the *Health Information Act,* and our office was invited to participate in that review. In early 2025 I provided written submissions addressing changes that might improve the functioning of the *Act*.

Lastly, the *Access to Information and Protection of Privacy Act* is subject to a review per section 74 of that *Act*. Following some general discussions with the Access and Privacy Office, in early 2025 I provided written submissions to the Department of Justice addressing potential changes.

Should the Legislative Assembly consider legislation to amend either the HIA or the ATIPPA, our office will be pleased to provide input if requested.

Section 23: Protecting Personal Information of Public Employees

Public bodies' records frequently contain personal information, and responding to requests for access to those records can involve a complicated analysis when the personal information belongs to someone other than the applicant. This is called "third-party personal information".

Governments act through their employees; records created by employees in the course of their employment are records of government information. Records revealing which government employee took an action or communicated a fact or opinion as part of their employment should generally not be viewed as the writer's personal information; rather, it should be understood as information about the government performing its duties through its employees.

Some recent files suggest that public bodies' employees are often unaware that the emails written in the course of employment are not the personal information of the email authors; rather, they are the public body's work product. There are numerous exceptions in the *Act* that allow a public body to refuse to disclose some or all of a record, and the protection against unreasonable invasion of personal privacy provided by section 23 is certainly available to protect public bodies employees' personal information. However, public bodies' employees must also be aware that their employer is fundamentally different than a private organization not subject to the *Act*. Employees who create records in their work for a public body – and this includes all who might write an email as part of their work – need to be mindful that the records they create are subject to the public right of access under the *Act*.

This is an ongoing concern that must be addressed through training.

Section 24.2: Information Created or Gathered for the Purpose of a Workplace Investigation

When the *Act* was amended in 2019, section 24.2 was added to govern how public bodies respond to requests for access to information that is created or gathered for the purpose of a workplace investigation. These records often contain very sensitive information about identifiable individuals. Section 24.2 places an absolute prohibition on disclosure of these records to anyone who is not a party to the investigation. However, the complainant and respondent in the investigation are entitled to access the relevant information that was created or gathered for the purpose of a workplace investigation, subject always to any other exceptions to disclosure in the *Act*. This strikes a balance between the need to protect the privacy of those involved in a workplace investigation and the right of access for parties.

A few reviews completed in 2024/2025 involved records that were created or gathered for a workplace investigation. In some of these cases, the public body explained redactions were required because witnesses had been told their statements were confidential and would never be disclosed. This is clearly not aligned with the requirements of section 24.2.

In early 2024 I inquired with the Labour Relations Unit at the Department of Finance what if any changes had been made to the conduct of workplace investigations to account for the change to the legislation. I was advised that there had been none, but there was an intention to consider the question before the end of the fiscal year. This is disappointing, given that there was a two year period between the amendment passing and then coming into force in July 2021, and there was a further 2½ year period after it had been in force. Section 24.2 made specific changes to the law governing access to information collected in the course of workplace investigations, and public bodies need to adapt their processes accordingly.

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

Review Reports

My office received 173 reports of privacy breaches from health information custodians this year. I issued 15 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 any recommendations that were made in a report to a health information custodian that were not accepted. We are pleased to report that all recommendations in the fifteen reviews were accepted.

Alternative Resolution

My office resolves most privacy breaches without issuing formal review reports. Typically, we will receive a notice of a breach from the health information custodian and later a final investigation report. We will then 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 some further information. We will provide comment and guidance on how to avoid similar breaches in the future, and we may identify relevant resources for consideration. Typically, these are instances where the likelihood of significant harm is low. Informal processes typically conclude faster than a formal review.

Generally speaking, health information custodians take privacy breaches seriously, even where the risk of harm is not high. Nevertheless, there continue to be instances where employees do not respond correctly to a privacy breach. This causes delay in notice to the affected individual, notice to my office, and completion of the investigation.

Implementing Recommendations in a Review Report - Oversight

A review report of a privacy breach 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 *Act* deems a failure to notify the Commissioner of the decision within 30 days as a decision *not* to follow the recommendations.[8] If a recommendation is accepted, the custodian must comply with the recommendation within 45 days.

The process is straightforward, but there is no oversight of the implementation of an accepted recommendation. Our office does not have any authority to conduct such oversight, nor is a custodian legally obliged to report on the implementation of any accepted recommendations. In

[8] Section 156.

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 2: *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.*

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

Incidence of Privacy Breaches

The number of new *Health Information Act* files increased significantly this year, from 78 to 180.

The Northwest Territories Health and Social Services Authority (NTHSSA) submitted most of the breach notices. This is to be expected: the NTHSSA provides health services to most communities in the Northwest Territories.

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

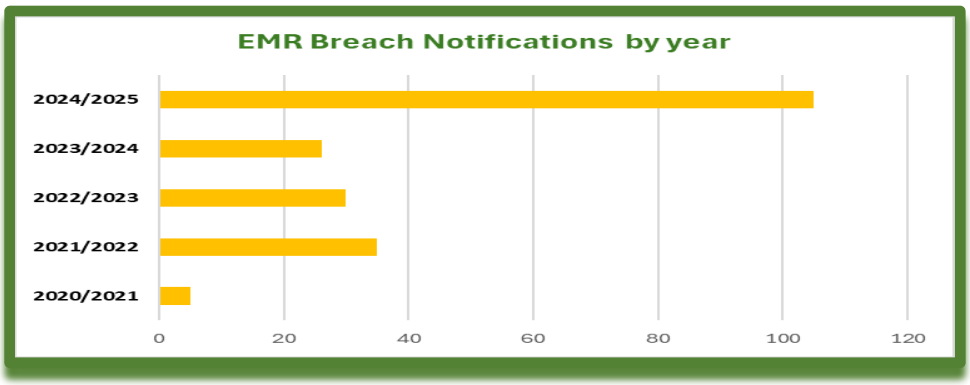
Almost all these breaches are caused by momentary inattention to detail while linking documents in the EMR, sending a fax, printing documents, or sending an email. Details are critical, both to protect patient privacy and to ensure patients' medical care is never compromised by information mismanagement. It follows that the employees must be provided the appropriate training and support.

[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.

Recurring Issues in Privacy Breaches

Scanning/Linking EMR Errors

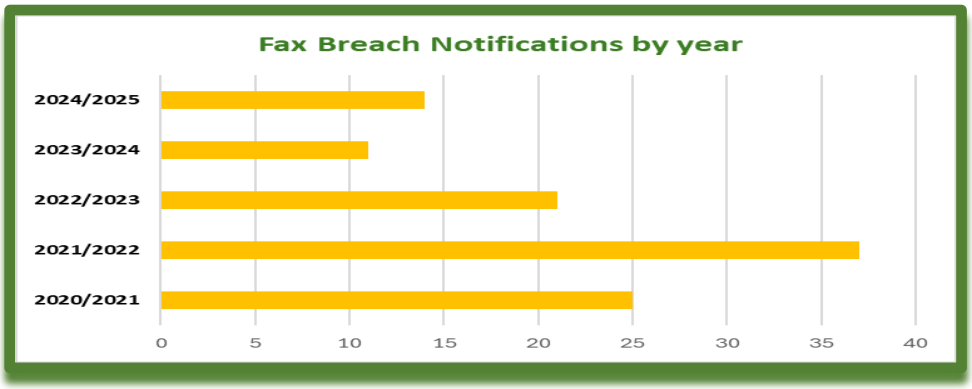
In 2024/2025, more than half of the privacy breach notifications involved scanning and linking errors within the EMR. These occur when personal health information is scanned into the EMR and then linked to the wrong patient's chart. This prevents the patient's care team from receiving the updates they need to do their jobs and discloses personal health information to the wrong health-care provider.



Faxing

Fax machines have been a significant factor in privacy breaches since the *Act* 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.



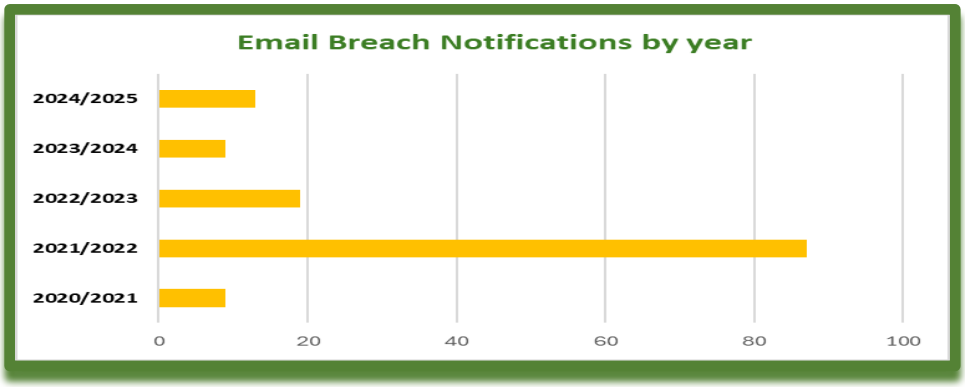
Recommendation 3: *Health information custodians should continue to reduce or eliminate the use of fax machines to transmit personal health information.*

Email

Privacy breaches often involve personal health information being sent 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.

Chain emails continued to contribute to privacy breaches in 2024/2025. A chain email can be an efficient and privacy-protective way to share information with a small group that needs it to do their jobs. Unfortunately, email chains tend to accumulate information as they pass from recipient to recipient, increasing the risk of a privacy breach if the message is forwarded to a person not anticipated by the original sender.

Regular privacy training for staff can remind them to apply passwords to documents or use secure file transfer. These measures reduce the chance that an unintended recipient will be able to access someone's personal information. Where group emails must be used to share information, the "bcc" function can prevent recipients from accidentally responding to the entire group.



Privacy Training

To prevent privacy breaches, a strong culture of privacy awareness and a keen sensitivity to privacy issues is essential. Training will help to create a privacy-protective workplace culture and avoid incidents that proceed from momentary inattention. Employees who work 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. It applies to the Department and the Health and Social Services Authorities, and it requires that 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 is to ensure employees are trained to prevent breaches and to respond to breaches appropriately.

Despite the policy, we still encounter privacy breaches involving employees who have not received privacy training. 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 4: *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 a final report is not received for several months more. The *HIA* requires notice to be provided as soon as reasonably possible.[10] 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 the requirement of notice. It requires notice only after a full investigation has confirmed a privacy breach occurred. This is not appropriate, as it is inconsistent with the *Act*'s 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.

The need for timely notice was the subject of a recommendation in last year's report and in at least one review report. In response, NTHSSA has developed and shared a draft procedure document addressing the various steps required for a privacy breach investigation. This draft procedure addresses the need for timely notice. We anticipate the final document will provide the clear direction needed.

[10] Section 87

Privacy Impact Assessments

Our office commented on Privacy Impact Assessments (PIAs) involving a cancer screening database, a digital imaging archiving and communication system, an on-line application for vital statistics certificates, and new chemistry analyzers with e-connectivity. We received additional information regarding existing PIAs for a health data repository and for the BDM Pharmacy System replacement.

Under the *HIA,* a PIA is used to identify privacy risks posed by new health care information or communication systems, or by changes to existing systems.[11] The *Act* allows the Commissioner to comment on a PIA,[12] ostensibly so the health information custodian can consider those comments when finalizing design and implementation plans. Ideally, a PIA should be provided for review at an early stage of project development so that any comments from the Commissioner can be considered and incorporated where appropriate.[13] For comparison, the *ATIPPA* now stipulates these requirements for PIAs.[14]

The Department did not accept past recommendations to adopt a policy requiring PIAs to be provided early or to receive and consider comments from the Commissioner. The Department has stated that it already prepares PIAs during the planning phase and also points 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*[15] would 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*.[16] A PIA is a planning tool to design privacy protection into information and communication systems; not an evaluation tool after a project is completed. Alternatively, the Privacy Impact Assessment Policy could be updated to address this concern.

Recommendation 5: *Privacy Impact Assessments (PIAs) 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 review of any comments by the health information custodian while the project or program is still in the planning stage.*

Recommendation 6: *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.*

---

[11] Section 89
[12] Section 175
[13] 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
[14] See section 42.1 of ATIPPA
[15] Per section 195.1, the *Health Information Act* is to be reviewed every 10 years. The Act came into force in 2015.
[16] This section was added in 2019 and came into force July 30, 2021.

Interjurisdictional Activity

The federal, provincial, and territorial Information and Privacy Commissioners meet 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 regular meetings are a valuable forum to stay informed of policy developments at the national and international level.

Commissioners met in person in Toronto in October 2024. After the two-day conference, we issued joint resolutions on transparency by default in government services, on responsible information-sharing in situations involving intimate partner violence, and on identifying and mitigating harms from privacy-related deceptive design patterns.

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*[17] *(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*.[18] With the amendments that came into force in 2021, municipalities may be designated as public bodies by regulation.[19]

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.[20]

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, 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.

[17] *SNWT 1994, c 20.*
[18] Subject to limitations and exceptions set under ATIPPA or other legislation.
[19] No communities have yet been designated.
[20] 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 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*[21] (*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[22] 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.[23] The Commissioner may initiate an investigation of a privacy breach upon the request of an individual who believes their personal health information was collected, used, or disclosed in contravention of the *Act*, or, in appropriate circumstances, the Commissioner may initiate a review independently. After conducting a review, the Commissioner will prepare a report and may make recommendations to the health information custodian. The health information custodian must notify the Commissioner of the health information custodian's decision to follow or not to follow the recommendation(s) 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.

[21] SNWT 2014, c 2.
[22] Section 87 of the *Health Information Act*.
[23] 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: *The Legislative Assembly should consider amending the ATIPPA to allow a public body to extend the time once for the period required to complete third-party consultation without authorization by the IPC. For subsequent extensions, public bodies should continue to seek authorization from the IPC. (Page 10)*

Recommendation 2: *The Department of Health and Social Services should consider implementing a policy, or the Legislative Assembly should consider amending the Health Information Act to require health information custodians to report to the Commissioner regarding the implementation of accepted recommendations. (Page 15)*

Recommendation 3: *Health information custodians should continue to reduce or eliminate the use of fax machines to transmit personal health information. (Page 17)*

Recommendation 4: *Health information custodians should prioritize implementation of, and compliance with, the Mandatory Training Policy and ensure that appropriate privacy training is provided for new employees, returning employees, and for all employees annually. (Page 18)*

Recommendation 5: *Privacy Impact Assessments (PIAs) 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 review of any comments by the health information custodian while the project or program is still in the planning stage. (Page 19)*

Recommendation 6: *The Legislative Assembly should consider amending section 89 of the Health Information Act to include similar provisions regarding Privacy Impact Assessments as mandated in section 42.1 of the ATIPPA. (Page 19)*

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