Northwest Territories

20/21

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NORTHWEST TERRITORIES

Annual Report

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

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

Kīspin ki nitawihtīn ē nīhīyawihk ōma ācimōwin, tipwāsinān.
Cree

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

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

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

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

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

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.
Inuvialuktun

ᑖᒃᑯᐊ ᑎᑎᖅᑲᐃᑦ ᐱᓕᒍᐁᐱᑦ ᐃᓄᒃᑎᑐᓪᓗᖅᓯᒪᓕᓂᑎᒃ, ᐅᖃᖅᑎᖅᓄᑦ ᐅᖅᑰᓕᕐᓇᖅᑐᑎᑦ.
Inuktitut

Hapkua titiqqat pijumagupkit Inuinnaqtun, uvaptinnut hivajarlutit.
Inuinnaqtun

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

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

July 1, 2021

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

Dear Mr. Speaker

Pursuant to section 68 of the *Access to Information and Protection of Privacy Act* and section 173 of the *Health Information Act,* I have the honour to submit my Annual Report to the Legislative Assembly of the Northwest Territories for the period from April 1, 2020, to March 31, 2021.

Your truly,

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

/af

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

Table of Contents

Commissioner's Message

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

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

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

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

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

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

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

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

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

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

Financial Report

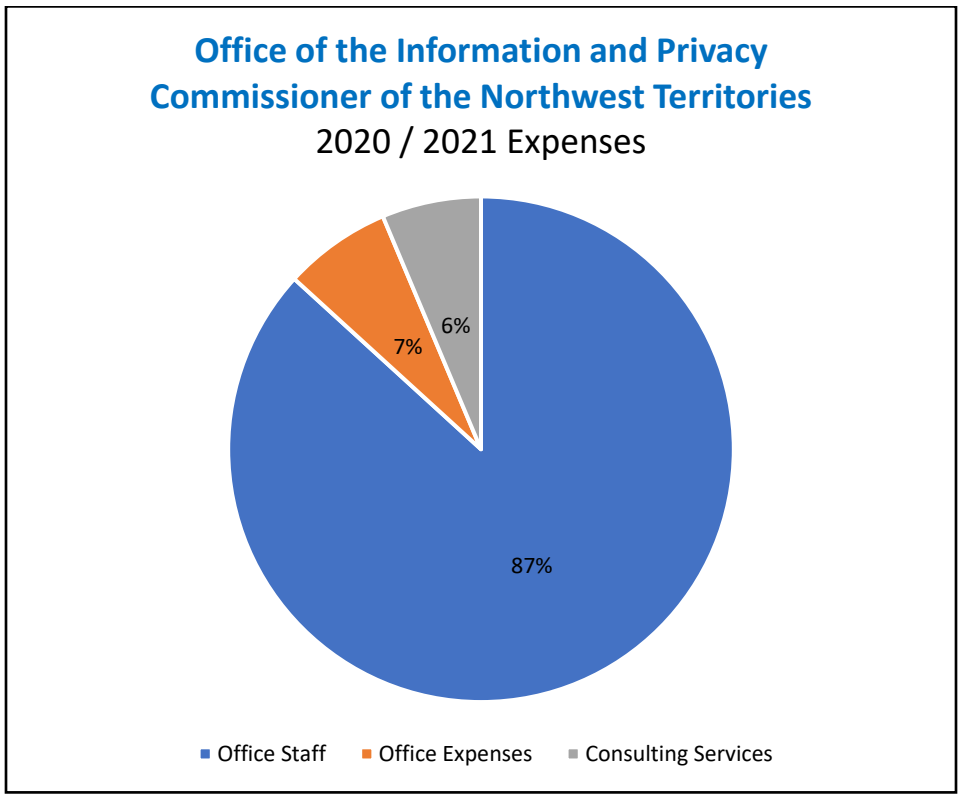
The total amount spent to operate the Office of the Information and Privacy Commissioner (OIPC) of the Northwest Territories for the fiscal year 2020/2021 was $547,168.63. A detailed breakdown is outlined in the charts on the next page.[1]

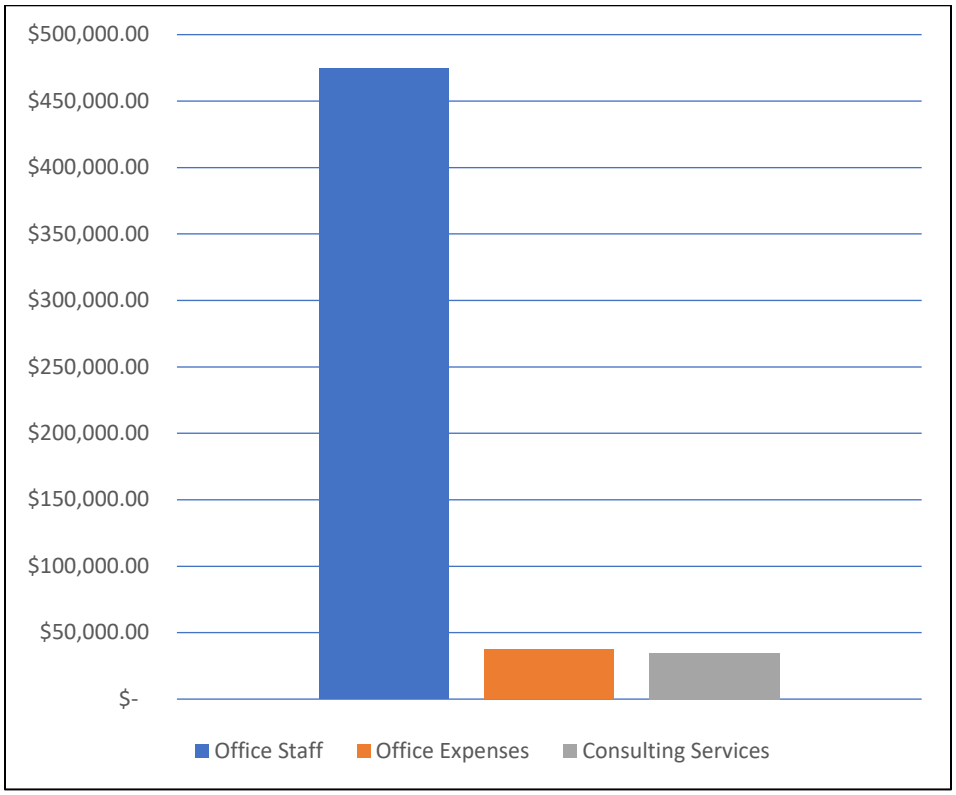
New computer hardware and software were installed in December of 2020. This immediately improved the utility and stability of the office systems. The OIPC is most grateful to the former Commissioner, Ms. Keenan Bengts, who prioritized this improvement! It has been of great assistance to all, both in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

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

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

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


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


$500,000.00
$450,000.00
$400,000.00
$350,000.00
$300,000.00
$250,000.00
$200,000.00
$150,000.00
$100,000.00
$50,000.00
$-
Office Staff
Office Expenses
Consulting Services

Office of the Information and Privacy Commissioner and Enabling Legislation

The *Access to Information and Protection of Privacy Act*

The *Access to Information and Protection of Privacy Act (ATIPPA)* applies to the departments, branches, and offices of the government of the Northwest Territories, plus 22 agencies, boards, commissions, corporations, and other public bodies designated in the regulations to the *Act*. The *ATIPP Act* enshrines four key rights and obligations:

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

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

The *Health Information Act*

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

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

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

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

The Information and Privacy Commissioner

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

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

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

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

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

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

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

The Year in Review

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

Access to Information and Protection of Privacy Act

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

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

Health Information Act

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

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

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

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

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

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

Review Report 20-226

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

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

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

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

Review Report 20-228

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

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

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

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

Review Report 20-229

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

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

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

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

Review Report 20-230

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

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

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

Review Reports - *Health Information Act*

Fourteen Review Reports were issued under the *Health Information Act* in 2020/2021. These reports, like those issued under the *Access to Information and Protection of Privacy Act*, are available on-line at https://www.canlii.org/en/nt/ntipc/ . The reports review various instances of unauthorized collection, use or disclosure of personal health information.

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

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

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

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

Review Report 20-HIA 24

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

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

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

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

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

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

Review Report 20-HIA 28

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

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

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

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

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

Review Report 20-HIA 30

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Review Report 20-HIA 32

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

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

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

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

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

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

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

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

Review Report 20-HIA 35

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Trends and Issues

Vaccine passports

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ATIPPA amendments coming into force

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

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

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

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

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

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

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

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

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

Breaches of Privacy under the *Health Information Act*

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

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

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

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

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

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

Timely Responses to the OIPC

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

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

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

Timely responses to access to information requests

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

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

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

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

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

Personal Mobile Audio and Video records

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

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

Final Word

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

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

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

Contact Us

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

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

Email: admin@atipp-nt.ca

Website: www.atipp-nt.ca

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