Northwest Territories

19/20

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NORTHWEST TERRITORIES

Annual Report

OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
NORTHWEST TERRITORIES

Website: atipp-nt.ca
Email: admin@atipp-nt.ca
Phone: 1-867-669-0976 | Toll free: 1-888-521-7088

Table of Contents

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

July 27, 2020

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

Dear Mr. Speaker

I have the honour to submit my annual report to the Legislative Assembly of the Northwest Territories for the period from April 1st, 2019 to March 31st, 2020.

Yours very truly,

Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories

/kb

COMMISSIONER'S MESSAGE

A Retrospective Looking Ahead

This will be my last Annual Report as the Information and Privacy Commissioner for the Northwest Territories as my term expires at the end of October, after almost 24 years in the position. What better time is there to reflect on where we've been and where we are headed?

When I began this work in 1997, I had no real appreciation of the nature of the work or how important the mandate of the office was. Nor was it in any way evident how it would evolve to play such a significant role in today's very different world. Twenty-four years ago the internet was in its infancy – there was no Facebook or Google or Siri. Email was not an acceptable means of business communication. Today, we live on the internet and information, particularly personal information, has become a valuable commodity, bought and sold by both legitimate and nefarious actors. Personal information is collected in ways and in quantities that could not have been in any way contemplated 24 years ago. As was demonstrated with the Cambridge Analytica revelations following the 2016 Presidential Election in the United States, our personal information is being gathered, analyzed, manipulated and sold as never before and mostly without our knowledge or true consent. When dealing with private business, we have some choice – if we're vigilant and careful, we can limit how much of our personal information we are willing to part with and in what circumstances. The same does not apply to many of our interactions with government. If we need medical assistance, we have to give up personal information to the health care provider. If we want to obtain an education, we have to give up our personal information to government. If we want a driver's license, we have to provide our personal information to the government. More than ever, we need to be able to trust that government will properly handle all of the personal information we provide in the course of daily life. We need government to protect our privacy.

Democracy also demands that the public is able to have access to public records – records which by definition belong to the public – to allow us to participate fully in the democratic process and to aid in making our governments more transparent and accountable. As recent history has demonstrated, this is even more vital in times of emergency. We have seen many examples of governments throughout the world taking unprecedented steps to deal with the current world pandemic and social unrest, and concerns for the future of both democracy and privacy have been triggered worldwide. The rights reflected in the *Access to Information and Protection of Privacy Act* represent a powerful tool to help ensure government transparency and accountability.

The last 24 years have seen ever increasing threats to access and privacy, which makes this legislation even more important today.

I was excited last summer when the Legislative Assembly passed *Bill 29, An Act to Amend the Access to Information and Protection of Privacy Act*. As I noted in last year's annual report, these amendments will dramatically change the access and privacy regime in the Northwest Territories. The Information and Privacy Commissioner will be given the power to make binding orders on government, rather than merely making recommendations. This is a quantum leap in terms of the strength of the legislation. This transition from "recommendations" to "orders" is timely as over the last several years I have, unfortunately, seen a waning commitment to compliance with the current legislation. Required time limitations are being missed, dismissed and just outright ignored. There have been instances in which public bodies have simply failed to respond in any way to applicants making access requests. They are also more and more often failing to respond to communications from our office. Submissions from public bodies have become less thorough and less helpful. It is my hope that when the amendments come into effect, they will spur public bodies in the Northwest Territories to devote adequate resources to compliance activities, if only because non-compliance will have far more significant and costly implications.

To be fair to those on the front lines in public bodies who are largely responsible for access and privacy matters – known as ATIPP Coordinators – these failings, at least from my perspective, stem from a lack of leadership commitment and ever decreasing resources being devoted to these positions, coupled with significantly decreased training being provided to ATIPP Coordinators. Many of the most experienced and knowledgeable ATIPP Coordinators within the GNWT have left those positions over the last year and they have been replaced by individuals who have little or no background in ATIPP and who are not being properly supported in their roles with adequate training. Nor are they provided the time or resources to fulfill this important function, being that ATIPP is often dealt with as an "off the side of your desk task". At the same time, the number and complexity of access to information requests and privacy breach complaints have skyrocketed, particularly in the last year, to the point that in some cases it would be impossible even for a well-trained ATIPP Coordinator to keep up with the demand, working full time on ATIPP issues. Many Coordinators, however, have other important duties as well and ATIPP does not get priority. These new, poorly trained ATIPP Coordinators are, therefore, struggling to even understand their role, let alone to apply the legislation. Part of the problem may be that with the amendments coming into force at some point, there is a perception that there is little to be gained by spending time and resources training people under the existing legislation. However, Bill 29 was passed in June of last year and as of the date of the writing of this report in August of 2020, there is no indication as to when the new provisions might come into effect. Furthermore, key members of the team who have been instrumental in the implementation plan are no longer part of the team. It is unclear when implementation or even partial implementation might happen. In the current circumstances, it could be another six months or even a year. It is simply not good enough to wait for the amendments to come into force before moving forward.

Public bodies need to step up and ensure proper training and sufficient resources are available for ATIPP Coordinators to do their jobs right now.

Our office was busier than it has ever been in 2019/2020. We opened 76 files under the Northwest Territories *Access to Information and Protection of Privacy Act*, up by 38% from 2018-2019. The more startling statistic, however, is the increase in the number of files opened under the *Health Information Act*, which went from 29 files in 2018/2019 to 86 files in 2019/2020 – a whopping 197% increase! These numbers, overall, represent a 93% increase of files opened.

The number of files opened, however, does not tell the whole story. Every year both access and privacy issues become more complex. As of April 1, 2020 this office is no longer responsible for oversight in relation to the Nunavut *Access to Information and Protection of Privacy Act*, which will free up some additional time for the NWT office. However, we continue to be significantly understaffed and have not been able to meet our six month time frame for completing review reports for at least the last 3 fiscal years. And when the new legislative scheme is implemented, it will bring significant increased responsibility for the OIPC. Quite apart from the change from making recommendations to making orders, the new legislation will also bring in new breach notification requirements for all public bodies, will require approval from the Information and Privacy Commissioner for extensions of time, will mandate the Office of the Information and Privacy Commissioner to provide public education and, significantly, will shorten the time allowed for completing a review report from six months to just over 4 months.

A formal "needs assessment" for the office was completed in the early winter and recommendations were made to increase both the administrative and the investigative staff numbers and I am very pleased that the latest budget allowed for an increase of at least one investigator and more administrative assistance. We are anxious to get those positions filled as soon as possible so that we can clear the backlog and allow the office to prepare to meet its expanded mandate.

All of this is to say that access and privacy are becoming more and more time consuming and complicated. This trend will continue and the resources available to address these issues will need to increase in lock step with the demand. It is no longer sufficient for larger public bodies to rely on part-time ATIPP Coordinators. More time, energy and resources will have to be dedicated to the hiring and retaining of well-trained employees with the requisite expertise required in today's reality.

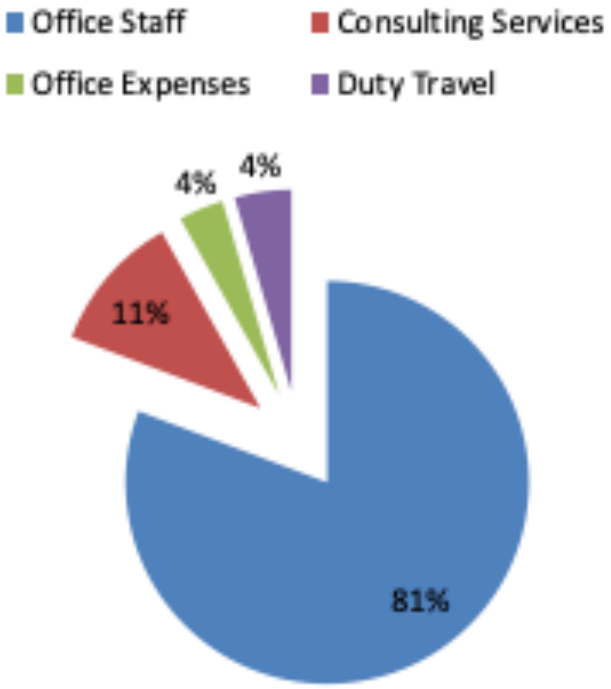
In closing, I would be remiss if I did not fully recognize and thank the OIPC staff, who are some of the best people I have ever had the pleasure of working with. Their enthusiasm, experience and dedication are second to none and the people of the Northwest Territories are exceedingly lucky to have them looking out for their rights. I would also like to sincerely thank the people of the Northwest Territories for putting their faith in me over the last 24 years. Being the Information and Privacy Commissioner of the Northwest Territories has been the most fulfilling job I have ever had and I hope I have left the new Information and Privacy Commissioner with a good foundation on which to build on the important work of this office.

FINANCIALS

Office of the Information and Privacy Commisioner of NT & NU Expenses for 2019-2020

The total (combined funds) spent to run the Offices of the Information and Privacy Commissioner for the Northwest Territories and for Nunavut for fiscal 2019/2020 was $395,144.40, the detailed breakdown for which is shown in the charts.

Office Staff	$319,084.82
Consulting Services	$43,953.25
Office Expenses	$14,185.37
Duty Travel	$17,920.96
TOTAL	$395,144.40



ABOUT THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

The Information and Privacy Commissioner is an Officer 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 performs the legislative and regulatory responsibilities set out in the *Access to Information and Protection of Privacy Act* (ATIPPA) and the *Health Information Act* (HIA).

Access to Information and Protection of Privacy Act

The *Access to Information and Protection of Privacy Act* applies to 32 territorial departments, crown corporations and other public agencies. The ATIPP Act enshrines three key principles:

- the right of the public to have access to any record 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; and
- the obligation of public bodies to protect the privacy of individuals by setting out the circumstances in which a public body may collect, use or disclose personal information.

It outlines the process for the public to obtain access to records and establishes when and how public bodies can collect, use or disclose personal information about individuals.

The Health Information Act

The *Health Information Act* (HIA) came into effect on October 1st, 2015. Its purpose is to govern the collection, use and disclosure of personal health information while recognizing the need to use and disclose such information as necessary to provide effective and efficient health care. The legislation applies to all records containing the personal health information of identifiable individuals in the custody or control of health information custodians as defined by the legislation. It regulates health information custodians in both the private and the public 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 Tlicho Community Services Agency, as well as private physicians and pharmacies operating in the Northwest Territories. HIA also applies to "agents," who perform a service for custodians, such as employees, contractors, students and volunteers. Custodians are responsible for the information collected, used and disclosed by their agents.

The HIA sets out the rules that health service providers must follow when collecting, using and disclosing personal health information. Over-arching all of these provisions is the clear direction that a medical care worker's access to any personal health information is to be limited to that information which the care provider "needs to know" to do their job.

The Act protects patients' privacy by regulating how health information may be collected, used and disclosed, and by establishing the duty for custodians to take reasonable steps to protect the confidentiality and security of health information. The Act also gives individuals the

right to access their own health information, and to request corrections to that information. It also gives the patient the right to put conditions on who has access to his or her personal health records and to direct, for example, that one or more practitioners, nurses, clerical staff or other employees in any particular office be prohibited from accessing that patient's records.

The *Health Information Act* also imposes a positive duty on health information custodians to give notice to an individual as well as to the Information and Privacy Commissioner if personal health information about the individual is used or disclosed contrary to the Act, or is stolen, lost, altered or improperly destroyed. The Information and Privacy Commissioner may conduct a review and prepare a report with appropriate recommendations in such circumstances.

TIMELINESS OF ACCESS

Timeliness of access is a vitally important principle. Surely it should go without saying that respect for the law is even more important ...

The all-time highs for requests undoubtedly present challenges and I credit the dedicated public servants, particularly those in the Information Access Operations office, who work very hard to keep pace. The fact is, however, that the public service must have the resources necessary to keep pace with demand and to comply with the law.

Excerpt from Special Report – Now is the time: A report card on government's access to information timeliness, OIPC BC, September 2, 2020

The Role of the Information and Privacy Commissioner

The Office of the Information and Privacy Commissioner provides independent oversight over the decisions made by public bodies and health information custodians in responding to access to information requests and investigates allegations of privacy breaches under both the *Access to Information and Protection of Privacy Act* and the *Health Information Act*.

When a public body or a health information custodian fails to respond adequately to a request for information, an Applicant is entitled to make a Request for Review to the Office of the Information and Privacy Commissioner for an independent review and assessment. Similarly, if an individual has a privacy concern that has not been addressed by a public body or a health information custodian, as the case may be, they may request that the Office of the Information and Privacy Commissioner conduct an independent review of the issues.

The Information and Privacy Commissioner investigates complaints by obtaining input from all parties concerned, and issues a report outlining her findings after assessing the information received and interpreting and applying the various sections of the legislation which apply. In the report, the Information and Privacy Commissioner will make recommendations to the public body or health information custodian, as the case may be. Public bodies and health information custodians are required to respond to recommendations made by the Information and Privacy

Commissioner but they are not currently required to accept the recommendations made. In the case of recommendations made under the *Health Information Act*, however, where a health information custodian does accept a recommendation, the acceptance becomes legally binding and the custodian has 45 days to implement the recommendation or the failure can be taken to the Supreme Court for enforcement purposes.

Review Reports issued by the Information and Privacy Commissioner are public records and the IPC is required to include in her Annual Report an indication of any recommendations made which have not been accepted.

With the coming into effect of Bill 29, as discussed above, the role of the Information and Privacy Commissioner will change such that she will have the power under the *Access to Information and Protection of Privacy Act* to make binding orders, enforceable in the Supreme Court of the Northwest Territories. This order making power will not apply to matters under the *Health Information Act*.

In addition to dealing with complaints, the Information and Privacy Commissioner also reviews and comments on draft legislation and on privacy impact assessments when requested to do so.

Meeting of Canada's Federal/Provincial/Territorial Information and Privacy Commissioners/Ombuds Charlottetown, PEI August, 2019

THE YEAR IN REVIEW

With a 93% increase in the number of files opened by the Office of the Information and Privacy Commissioner of the Northwest Territories in fiscal 2019/2020 it was, by any measure, a record breaking year.

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT

Seventy-six files were opened under the *Access to Information and Protection of Privacy Act* between April 1st, 2019 and March 31st, 2020. These can be broken down into a number of categories:

Access to Information

- Review of Responses to ATIPP Requests . . 16
- Deemed Refusals 7
- Extensions of Time 2
- Third Party Requests 1

Privacy Issues

- Privacy Breach Complaints 27
- Breach Notifications from Public Bodies 5

Comments

- Requests for Comment from Public Bodies . 8
- Requests for Comments from members of the public 5
- Commissioner initiated comments 2

Miscellaneous

- Speaking Engagements 2
- Administrative 1

Clearly, privacy issues represented a significant portion of the requests for review in this time frame. The 27 privacy breach complaints this year far exceeds the six received in 2018-2019. It is the first time that privacy related files have outnumbered access to information matters. There is no clear indication as to why this might be the case, other than a public becoming increasingly aware and protective of their personal privacy. The number of deemed refusal files (where the public body has failed to respond to a request for information within the 30 days provided for in the *Act*) and the extension of time files (where the public body has taken an extension of the 30 day response period under section 11) continue to be concerning. As noted in both last year's Annual Report and in my opening comments in this report, this is an indication that there is a growing lack of capacity within public bodies to respond to access to information requests and points to a need for further resources and better training of ATIPP Coordinators.

In addition to the matters resulting in the opening of a file, we have, of course, also dealt with many calls on a daily basis from people seeking basic information about the *Act*, which we deal with immediately and without the need to open a file.

HEALTH INFORMATION ACT

Fiscal 2019-2020 saw a literal explosion of files opened under the *Health Information Act* with a total of 86 new files, compared to only 29 opened in 2018-2019.

Breach Notifications 58

Third Party Breach Notification (Saskatchewan Health) 1

Privacy Breach Complaints 8

PIA Reviews. 11

Commissioner Initiated Inquiries 6

Speaking Engagements. 1

Administrative. 1

Most of the breach notifications were received from the Northwest Territories Health and Social Services Authority (NTHSSA), which is to be expected in that most health services in the Northwest Territories are provided by this organization. It also attests to the fact that this organization is better at recognizing and reporting these breaches than other health information custodians. In this respect, I acknowledge and appreciate that NTHSSA has clearly been doing a better job of recognizing when privacy errors have been made.

Most of the breach notifications received involved one or two patients, and were, therefore, limited in scope. This was not, however, true of all breaches reported. Several of them involved large numbers of individuals and these are obviously more concerning.

Also concerning is the number of the reported breaches which resulted from the failure of employees to follow protocols requiring every patient to be identified with two points of identification (for example, a name and a birth date). In one incident, a patient was misidentified at least four times - when he made his appointment, when he checked in for his appointment, when he met with the physician and when the physician gave him a prescription. He and a relative had the same first and last names, and all of the clinical staff who dealt with him failed to recognize that they were referring to the relative's chart until the patient himself received the prescription, saw the error, and brought the error to the attention of health care providers.

Another common cause of privacy breaches has been the misdirection of documents by fax and by email. There have also been a surprising number of incidents in which a record containing personal health information has been sent to be printed on the wrong printer.

This office spent, quite literally, hundreds of hours reviewing and providing comments on a number of Privacy Impact Assessments (PIAs) submitted to our office pursuant to section 89(3) of the *Health Information Act* this past year. The *Health Information Act* requires health information custodians to "prepare a privacy impact assessment in respect of a proposed new, or a proposed change to an information system or communication technology relating to the collection, use or disclosure of personal health information". The legislation also provides that the Information and Privacy Commissioner may provide comment on PIAs received. The Act is, however, unfortunately silent on what, if anything, health information custodians should do when they receive comments from the Information and Commissioner. We have taken the position that the intention of the legislators was that PIAs should be prepared well in advance of implementation of new programs, that the Information and Privacy Commissioner should

review PIAs received with a view to making comments, suggestions and recommendations, and that the health information custodians responsible for the new programs or systems are then expected to take those comments and, at the very least, acknowledge the questions and concerns raised. The Department of Health and Social Services, however, takes a different view. Most, if not all of the PIAs received by the OIPC have been provided weeks and months after "go-live", though in one case, we did receive a PIA on a Friday at 5 p.m. for a system going live on Monday at 8 AM. I have also been provided with a PIA in which the analysis clearly indicated that the solution had unacceptable privacy impacts in accordance with current GNWT policy directives. Notwithstanding this, the new system had gone live with all of the attendant privacy risks and was active by the time my office received the PIA. With respect to one PIA recently reviewed by this office, when I asked for additional information including supporting documentation referred to in the document, I was told rather bluntly by the Chief Health Privacy Officer of the Department that my requests for more information "expanded" beyond my jurisdiction and that the "scope and depth" of comments I provided to PIAs submitted to my office far exceeded my office's role. I was also told that I have no mandate to comment on PIAs and that the Department has met its "legislative obligation by delivering a copy of the complete PIA" to my office.

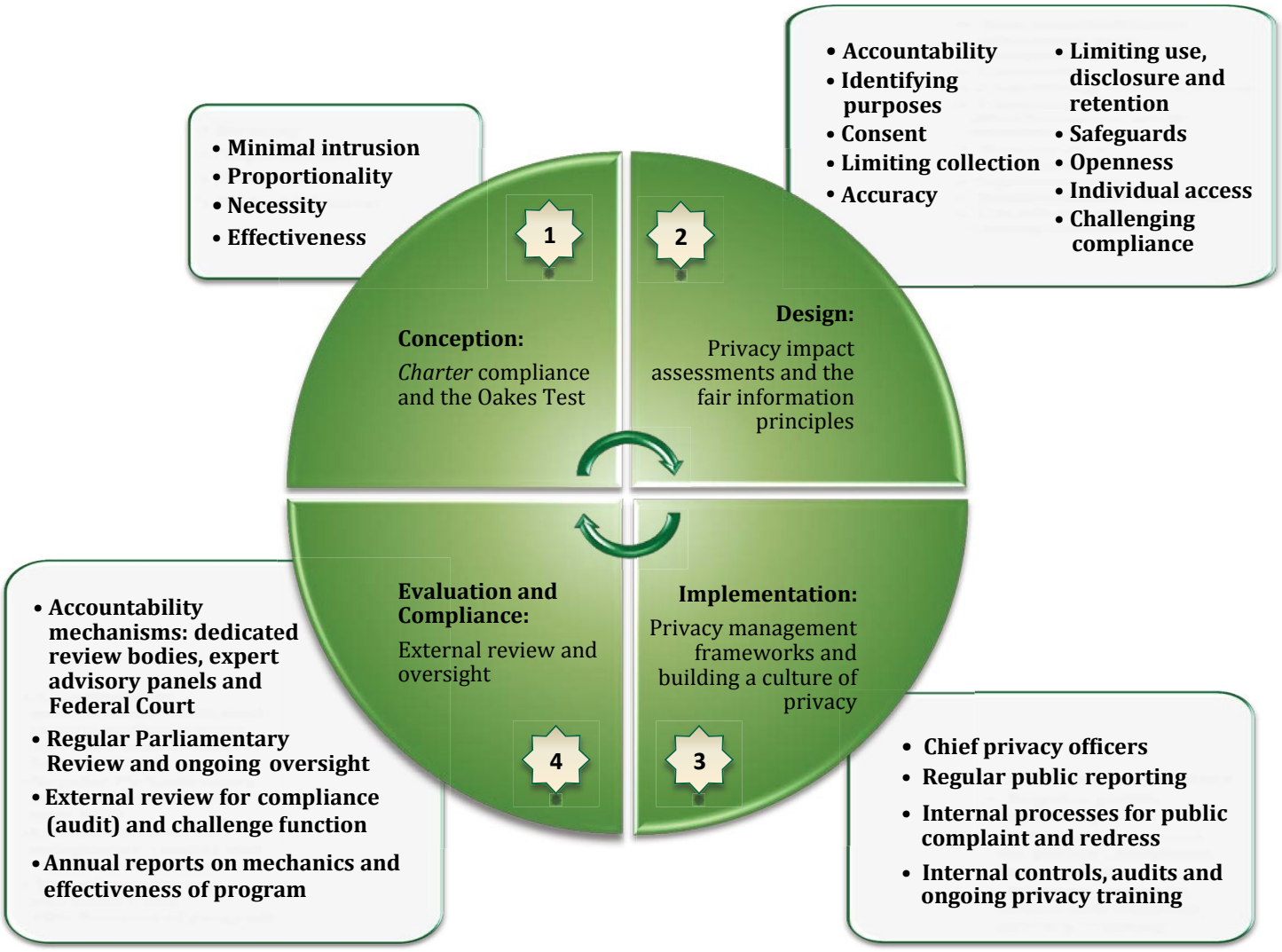
In my opinion, there must have been a purpose in requiring PIAs to be provided to the Information and Privacy Commissioner when this was included in the HIA.

We have since met with the Assistant Deputy Minister and the Chief Information Officer to discuss this issue and it is our hope that the Department will reconsider its interpretation of the PIA provisions of the HIA.

We consider PIAs to be a vital component in the planning and implementation of new systems and that they need to be given the attention they deserve. They are not merely for the purpose of checking a box that says "we prepared a PIA and sent it to the IPC".

Privacy from the start: four stages for consideration

There are four general stages — conception, design, implementation and evaluation — in the development and implementation of security programs and policies. In each of these stages, there are certain factors that should be taken into account in order to ensure that privacy is respected and carefully documented (as within Privacy Impact Assessments).



This diagram copied from – A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century – A Reference Document from the Office of the Privacy Commissioner of Canada. Available at https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_sec_201011/#toc2

REVIEW REPORTS

Twenty seven Review Reports were issued under the *Access to Information and Protection of Privacy Act* in 2019-2020

Review Report 19-196

Category of Review: Access to Information

Public Body Involved: Department of Health and Social Services

Sections of the Act Applied:
Sections 16(1)(c), 24(1)(b), 24(1)(c),

Outcome: Recommendations accepted

This matter arose out of a request for information about a research study on the impact of alcohol warning labels. The Department withheld access to all responsive records, with the exception of 5 pages which were partially withheld. The Department relied on sections 24 (business interests of third parties), 23 (unreasonable invasion of privacy), and section 16 (impairment of intergovernmental relations).

The Information and Privacy Commissioner (IPC) reviewed all relevant sections of the legislation, including section 5(2) which requires that where information excepted from disclosure can be reasonably severed, the remainder of the record must be disclosed. The IPC was not convinced that the disclosure of the information in question could reasonably be expected to impair the GNWT's intergovernmental relationship with the Government of Ontario, who objected to the disclosure. She did find that some of the information fit the criteria for an exception to disclosure as "financial, scientific, technical or labour relations information obtained in confidence from a third party" and was appropriately withheld pursuant to section 24. The IPC recommended the disclosure of most of the records in question with some exceptions.

Review Report 19-197

Category of Review: Access to Information

Public Body Involved: Department of Environment and Natural Resources

Sections of the Act Applied:
Section 1, Section 2 (personal information), Section 5, Section 23(2)(d), Section 23(4),

Outcome: Recommendations accepted

The Applicant requested access to records in relation to an incident involving wildlife at a remote worksite. Access to most records was denied on the basis that the information was the personal information of a third party and that disclosure was prohibited by section 23(2)(d) which raises a presumption that disclosure of personal information amounts to an unreasonable invasion of privacy where the information was compiled and is identifiable as part of an investigation into a possible contravention of law. In this case, there was an active and ongoing investigation into the incident and it was anticipated that charges would be laid.

The IPC found that to the extent that information redacted related to the employment responsibilities of a GNWT employee, the disclosure did not amount to an unreasonable invasion of privacy (section 23(4)). She further found that section 23(2)(d) did not apply to information in relation to a business or other organization, but only to individuals. The records were reviewed page by page and line by line and the IPC recommended the disclosure of large portions of the records withheld.

Review Report 19-198

Category of Review: Access to Information

Public Body Involved: Northwest Territories Health and Social Services Authority

Sections of the Act Applied:
Section 1, Section 7, Section 14(1)(b)

Outcome: Recommendations accepted

The Applicant was an employee of the NTHSSA and had been involved in a workplace dispute. He requested access to copies of "shadow" files about him in the possession of seven named employees as well as emails between those same employees in which he was mentioned. The Applicant alleged that the public body had not provided all responsive records. He was also concerned by what he felt were indications that not all records of a disciplinary nature were being properly recorded in his formal personnel file but that there were "shadow" files in which managers kept their own records. He also argued that the public body did not properly apply section 14 which allows public bodies to withhold information that would reveal consultations or deliberations among GNWT employees.

The IPC commented on the practice of having employees search their own records in situations in which there is an actual or perceived conflict of interest and the reliance on untrained individuals to identify responsive records. She recommended that a second, more thorough search for documents be conducted. She identified that some attachments to emails did not appear to have been disclosed and recommended the disclosure of these records, subject to appropriate vetting. She reviewed all records for which section 14 had been applied and recommended the disclosure of much of the information withheld pursuant to this exception. She also made recommendations with respect to policies and procedures around the collection and maintenance of information that relates to personnel performance to ensure adequate security is in place to prevent unauthorized access to those records.

Review Report 19-199

Category of Review: Access to Information

Public Body Involved: Department of Health and Social Services

Sections of the Act Applied:
Section 3, Section 4, Section 5(2), Section 23

Outcome: Recommendations accepted

An applicant made a request for information about complaints made about licensed and/or unlicensed psychologists in the Northwest Territories over a six year period. The Department identified three such complaints but refused to disclose any of the responsive records on the basis that

a) at the time of the request, the Department had "care or control" of the records in relation to only one of the three complaints because the two other files were open files and all relevant documents had been handed over to the Complaints Officer; and

b) to disclose the records would amount to an unreasonable invasion of privacy.

The IPC found that the Department continued to have "control" of the records notwithstanding that they had been given to an agent to conduct an investigation. She further found that the lack of a legislatively mandated complaints registry was not a barrier to disclosure because the ATIPP Act clearly applied to the records, whether or not a registry existed. Finally, the IPC agreed that the records for the one file that were made available did contain sensitive personal

information but found that the records could be effectively redacted so as to remove personally identifying information and that the balance of the information could be disclosed and recommended such disclosure.

Review Report 19-200

Category of Review: Access to Information Request - Deemed Refusal

Public Body Involved: Department of Finance (Human Resources)

Sections of the Act Applied: Section 1, Section 6(3), Section 7(1), Section 8, Section 11,

Outcomes:
Recommendation to have dedicated ATIPP Coordinator not accepted

Recommendation to review processes accepted in part

The Applicant made a request for his own personal information from the Department of Finance on July 23, 2018. On August 17th, the Department wrote to the Applicant extending the time for responding to the request to October 1st. No response was received by October 3rd and the Applicant sought a review on the basis of a deemed refusal. The IPC attempted to resolve the matter without a review, but on October 11th, the Department advised that they were not in a position to respond within the time frame provided by the IPC. The Information and Privacy Commissioner therefore commenced a review on the basis of a deemed refusal under section 8 of the Act and requested submissions. The Department continued to miss deadlines imposed by the IPC but finally responded to the Applicant's request on January 10th, 2019.

The IPC found that the Department had failed in their duty to assist the Applicant (section 7) and, while the initial extension of time was reasonable and dealt with as required by the Act, the extended time period was not met and the Department failed to communicate effectively with the Applicant or with the office of the IPC. She commented on the turn-over in the ATIPP Coordinator position within the Department (3 Coordinators during the 6 months this matter was ongoing) and the apparent lack of experience or expertise for dealing with access requests within the organization.

The IPC recommended that the Department establish a dedicated, full time position of ATIPP Coordinator with the necessary experience and expertise necessary to respond to access requests. She further recommended that the Department review its processes in relation to responding to ATIPP requests.

> This was a fairly complex request involving a lot of records from a number of employees. A timely response would require a degree of expertise. That expertise clearly did not exist and was a major factor in the delay.
>
> **Review Report 19-200**

Review Report 19-201

Category of Review: Access to Information

Public Body Involved: Department of Industry, Tourism and Investment

Sections of the Act Applied: Section 7, Section 10, Section 14(1) and Section 23

Outcome: Recommendations largely accepted

The Applicant requested a copy of a report resulting from a sole source contract, including all correspondence related to the handling and processing of the access to information request.

The public body identified and disclosed records responsive to the request but redacted some information pursuant to sections 14 (advice, recommendations, consultations and deliberations) and 23 (unreasonable invasion of third party privacy). The Applicant sought a review of the information withheld. He was also concerned because his name had been disclosed to those searching for responsive records.

The IPC found that most of the redactions had been properly applied under the Act, but recommended the disclosure of some additional information. She also recommended that steps be taken to protect the name of Applicants, when possible.

Review Report 19-202

Category of Review: Access to Information - Deemed Refusal

Public Body Involved: Department of Finance

Sections of the Act Applied: Section 7, Section 8, Section 11

Outcome: Recommendations largely accepted

The Applicant made a request to the Department of Health and Social Services for his own personal information. That request was transferred by the Department to the Northwest Territories Health and Social Services Authority who in turn transferred part of the request to the Department of Finance. The Department of Finance did not acknowledge the transfer. After several follow up emails from the Applicant with no response, the Department acknowledged, more than two months after the request had been transferred to them, that they were "actioning" the request. After two more months and several more emails with no further response, on September 14, 2018 the Applicant requested a review by the OIPC on the basis of a deemed refusal. The IPC wrote to the Department on October 2nd, and October 29th requesting information for the review. On November 2nd, the Department advised the IPC that the responsive records had been identified but had not yet been reviewed but would be available by November 12th. On November 15th the Department acknowledged to the IPC that the Request for Information had been received on May 24th but that as a result of an internal administrative error, it had not been recorded as having been received, resulting in confusion and delays. A partial response was received by the Applicant on November 27th and a final disclosure occurred on December 27th. In dealing only with the delay issue, the IPC found that the Department failed to meet its duty to assist and, in fact, actively ignored the request for extended periods of time and that it failed to cooperate with the IPC in the review process. The Department also failed to properly extend the time for responding, simply ignoring all requirements the Act. The IPC recommended a review of its organizational chart to ensure that those tasked with responding to access requests are not over-burdened with other job responsibilities and that sufficient resources are committed to the Department's legislated responsibilities under the Act. She also recommended that ATIPP Coordinators be provided with adequate training to be able to effectively and efficiently respond to ATIPP requests and that a written register of ATIPP requests be maintained. A recommendation was also made that the Department review its policies and processes.

Review Report 19-203

Category of Review: Access to Information

Public Bodies Involved:
Department of Health and Social Services

Northwest Territories Health and Social Services Authority

Sections of the Act Applied: Section 1, Section 34, Section 56(1)

Outcome: Recommendation not accepted

The Applicant requested information about racism, cultural/racial bias in the healthcare system and the results and findings of an external investigation into a specific individual's death. A report was identified as being responsive to the second part of the request, but it was identified as a "critical incident report" completed in accordance with s. 25.3 of the *Hospital Insurance and Health and Social Services Act* (HIHSSA). NTHSSA refused to produce the report to the IPC for her review arguing that critical incident reports were excluded from the scope of ATIPPA. The IPC found that section 25.4(2) of the HIHSSA protected critical incident reports from being disclosed to the public, but did not prevent the IPC from reviewing such reports to confirm that they did, in fact, meet the criteria to be considered a critical incident report. The IPC recommended that the Department provide her with a copy of the record in question for the purposes of completing her review.

Review Report 19-204

Category of Review: Breach Notification

Public Body Involved: Hay River Health and Social Services Authority

Sections of the Act Applied: Section 4, Section 49.2

Outcome: Recommendations acknowledged and largely accepted

Hay River Health and Social Services Authority (HRHSSA) advised of a breach of privacy occasioned by the loss of a minor's health and social services file. The file contained very sensitive personal information about the child, his parents, his foster parents and possibly about others. The IPC found that the applicable legislation in this case was the *Access to Information and Protection of Privacy Act* because section 4(1)(a) of the *Health Information Act* specifically states that it does not apply to records relating to the administration of the *Child and Family Services Act*. She also found that the "notwithstanding" clause in the *Child and Family Services Act* did not oust the privacy protections for personal information contained in the ATIPP Act.

The IPC also commented that, while HRHSSA recognized that the breach affected the child, they did not recognize that it also affected the privacy of the foster parents and the parents of the child. Further, the IPC questioned whether it was appropriate for notice of the breach to be given to the foster parents as agents for the child instead of to the legal guardian, the Director of Child and Family Services. Further, both the foster parents and the parents of the child should have been given notice of the breach insofar as it affected their privacy. She also criticized HRHSSA for the lengthy delay in reporting the breach to the OPIC.

There were also issues with the Authority's response to the OIPC in that it required three letters and more than 3 months for the Authority to respond to correspondence from the OIPC and the response received did not contain the necessary level of detail to allow the OIPC to assess the nature of the breach or the response to it.

Recommendations were made that HRHSSA review its policies and procedures, in particular their Privacy Breach Policy and to ensure that it is

publicly available and that it is enforced. The IPC further recommended that a new policy be developed to address the physical and technical safeguards required for the storing of sensitive social services client files. Recommendations were also made with respect to notifications to be made to the affected parties.

Review Report 19-205

Category of Review: Access to Information

Public Body Involved: Northwest Territories Housing Corporation

Sections of the Act Applied: Section 1, Section 5(1), Section 7(1) and (2)

Outcome: Recommendation accepted

The Applicant made a request for a copy of the information that the Northwest Territories Housing Corporation receives each year from Canada Revenue Agency in order to calculate his rent. The Housing Corporation declined the request on the basis that the MOU they have with CRA prohibits such disclosure.

The IPC found that the MOU did prohibit the disclosure of information collected from the CRA for the purposes of administering its programs to any third party but that the Applicant was not a third party in relation to his own personal information. Alternatively, if he is a third party as contemplated in the MOU, there are provisions in the MOU which provide that the public body can request permission from CRA to disclose information to any third party with the consent of the individual the information is about.

The IPC recommended the disclosure of the information requested.

> In my opinion, when an individual is asking for his/her own personal information, that individual is not a third party - he/she is the owner of the information.
>
> **Review Report 19-205**

Review Report 19-206

Category of Review: Access to Information

Public Body Involved: Department of Health and Social Services

Sections of the Act Applied: Section 9, Section 14(1)(a), Section 16(1)(a), Section 17(1)(c)

Outcome: Recommendation accepted

A request was made to the Department of Health and Social Services for copies of briefing notes prepared for the Minister and the Deputy Minister concerning an agreement between Canadian jurisdictions with respect to pharmaceuticals.

The Department refused to disclose the requested information for on several grounds, including that the information in the responsive records constituted “advice, recommendations, policy options or proposals” (section 14(1)(a)), that disclosure would be reasonably expected to impair intergovernmental relations (section 16(1)(a)) and that disclosure would be reasonably expected to harm the economic interests of the Northwest Territories government (section 17(1)(c)).

The IPC found that the Department had properly applied Sections 16 and 17, but that section 14 did not apply and recommended the disclosure of some factual information.

Review Report 19-207

Category of Review: Access to Information

Public Body Involved: Department of Health and Social Services

Sections of the Act Applied: Section 3(1), Section 3(b.1), Section 4, Section 32, Section 33, Section 34

Outcome: Recommendation not accepted.

The Applicant sought copies of internal communications in relation to racism and cultural bias in the health system as well as the results and findings of an external investigation into a specific individual's death. The Department took the position that the external report was a "critical incident investigation" done in accordance with Section 25.3 of the *Hospital Insurance and Health and Social Services Act* (HIHSSA) and was not, therefore, subject to an access to information request. The Department also refused to share the report with the Information and Privacy Commissioner for the purposes of the review.

The Department took the position that section 25.4(2) of HISSA prevented the disclosure of any information in a notification or report or any information gathered, recorded or produced by or for the purpose of investigating a critical incident to "any person" other than those specifically named in the section. This section, they argued, prohibited the disclosure of the report to the Information and Privacy Commissioner as well as to the Applicant.

The IPC found that, because the onus of establishing that an applicant has no right to access to a record, they must establish that the record met the definition of the material described in section 35.4(2) of HISSA. The Department provided nothing other than their opinion that this was so, despite several attempts on the part of the IPC to obtain additional information about the record. The Department did not, therefore, meet the onus of establishing that the Applicant was not entitled to the record and the IPC therefore felt there was no option but to recommend that the records be disclosed in full.

Review Report 19-208

Category of Review: Access to Information

Public Body Involved: Department of Finance

Sections of the Act Applied: Section 15(a), Section 33

Outcome: Recommendations not accepted

This request for information involved a large number of records which were withheld pursuant to section 15(c) which provides public bodies with the discretion to refuse to disclose "information that is subject to any type of privilege available at law, including solicitor-client privilege". The IPC, as part of the review process, requested the confidential production of the records for which privilege was claimed so that she could properly analyze and assess the Department's claim of privilege. The Department, through its counsel, refused to produce the records for the Commissioner's review or to provide adequate affidavit evidence to support their claim.

Because the Department refused to provide the records to the IPC for assessment, that assessment had to be made on the basis of other evidence available. She reviewed the law with respect to solicitor-client privilege and applied that law to the evidence submitted by the Department for the purposes of the review. She found that the Department had not provided sufficient justification for its solicitor-client privilege claim. As a result, the public body had

not met the onus of establishing that the Applicant had no right to access to the records in question and the IPC therefore recommended that the records be disclosed in full.

The IPC also noted the government's failure to provide the records for her review jeopardizes the timely and cost-effective resolution of disputes and risks the government failing to make its case for privilege, when a review by the IPC of the disputed records could have led to a different outcome.

> The effective functioning of the system of independent review that the Legislature has established in the Act to a material degree depends on my Office being able to appropriately review disputed records. This is also true where solicitor client privilege is claimed. My ability to independently and efficiently verify the government's assertion of privilege maintains public trust and confidence in access to information in the Northwest Territories.
>
> **Review Report 19-208**

Review Report 19-209

Category of Review: Access to Information - Deemed Refusal

Public Body Involved: Department of Finance

Sections of the Act Applied: Section 7, Section 8, Section 11,

Outcome: Recommendations acknowledged but not clearly accepted

The Applicant made a request for information from the Department of Finance on January 11th, 2018. On February 6th, the Department advised the Applicant that, because of a large volume of records at issue (approximately 375 pages) the time for responding to the request was being extended to March 11th pursuant to section 11(b) of the Act. On March 6th, the Applicant contacted the public body to inquire as to the status of the matter, and again on March 19th. On April 3rd, the Applicant received a call from a new ATIPP Coordinator who indicated that the request would take an additional "week or two". On May 14th, the Applicant again contacted the public body for an update. He made three additional attempts to obtain an update during the month of May. Having still received no response by June 28th, 2018, the Applicant sought a review based on deemed refusal. The response to the Applicant's request was finally provided on July 19th, 2018.

The IPC found that the Department failed to respond to the request for information within 30 days of the request, or within the extended time frame taken by the public body pursuant to section 11 resulting in a "deemed refusal". She further found that the extension of time taken was not justified in that 375 pages of records could not, by any definition, be considered to be a "large volume" of records such that disclosure within the initial 30 day time frame would have "unreasonably interfered" with the department's operations.

The IPC made recommendations with respect to process and training for ATIPP Coordinators in the Department, and the review and development of policies and procedures.

Review Report 19-210

Category of Review: Access to Information

Public Body Involved: Department of Finance

Sections of the Act Applied: Section 1, Section 5, Section 7, Section 14(1)(c), Section 17(1)(c)(iii), Section 24, Section 25, Section 33

Outcome: Recommendations accepted

The Applicant requested specific information from the Department of Finance in relation to agreements signed with suppliers of cannabis products to the NWT Liquor and Cannabis Commission. Access to most of the responsive records was denied pursuant to sections 14(1)(c) (positions, plans, procedures etc. developed for contractual negotiations), 17(1)(c)(iii) (economic interests of the GNWT) and 25 (info required to be made available within 6 months).

The IPC reviewed the criteria for exceptions to disclosure as provided for in Sections 14 and 17 and recommended disclosure of significant portions of the records withheld. She further held that section 25 did not apply so as to allow the public body to avoid disclosing it because in this case, there was no "requirement" for the publication of the information in question, merely an intention to do so. Furthermore, the information eventually disclosed pro-actively by the public body was not fully responsive to the request made.

Review Report 19-211

Category of Review: Access to Information

Public Body Involved: Industry, Tourism and Investment

Sections of the Act Applied: Section 14, Section 23

Outcome:
Recommendations accepted except for three items withheld pursuant to section 14(1)

The Applicant made a request for information in relation to a particular contract with the International Institute for Sustainable Development. Partial access to the responsive records was provided but some information was withheld pursuant to sections 14 (advice, proposals and recommendations), and 23 (unreasonable invasion of privacy).

The IPC reviewed the records in question and recommended the disclosure of additional information. In particular, the IPC found that it was not an unreasonable invasion of privacy to reveal the names of the authors of a report when those individuals were contractors of the GNWT which brought them within the definition of "employee" in the Act. Section 23(4) specifically provides that it is not an unreasonable invasion of privacy to disclose information about the employment responsibilities of an employee. She noted that the public should be entitled to know who is authoring reports which have the potential to influence government decisions. She further found that much of the information withheld pursuant to section 14 did not meet the criteria for the exception to apply.

Review Report 20-212

Category of Review: Breach of Privacy Complaint

Public Body Involved: Department of Finance

Sections of the Act Applied: Section 42, Section 43, Section 47, Section 47.1

Outcome: No response received

The Applicant asked the OIPC to investigate whether there had been a breach of his privacy by a GNWT employee working in the Department of Finance. The Applicant was a health professional providing services to a client (AA). AA told the Complainant that his former life partner (BB), an employee of the Department of Finance, had given AA significant and detailed information about the Complainant, including information about the Complainant's education and employment history, his specific remuneration, and details about medical travel the Complainant had recently done. This information was imparted to AA in an apparent attempt to cause AA to lose trust in the Complainant as a health care professional.

The Department's investigation found that there was not sufficient evidence to conclude that the source of AA's information was the public body in general or BB in particular. The IPC disagreed with these conclusions and found that the Complainant's privacy had been breached and that, on a balance of probabilities, BB was the source of the disclosure, noting that BB had access to significant amounts of the Complainant's personal information by reason of BB's job responsibilities.

The IPC recommended that steps be taken to better secure personal information from unauthorized use within the department, including instituting periodic random audits to dissuade employees from inappropriate snooping. She also recommended that when allegations of privacy breaches are made, investigators chosen to investigate those allegations be unbiased and well versed in privacy law.

Review Report 20-213

Category of Review: Access to Information

Public Body Involved: Department of Infrastructure

Sections of the Act Applied: Section 23,

Outcome: Recommendation to disclose name of Third Party Employee not accepted

Recommendation to disclose "unresponsive" information accepted but reasoning rejected

The Applicant sought information about the land acknowledgment sign erected by the Northwest Territories Métis Nation at the junction of Highways 2 and 5. The public body provided a small package of responsive records, redacted to remove the names of non-employee third parties and, in one instance, a paragraph of an email on the basis that it was "not relevant" to the request.

The IPC found that the names of the individuals redacted from the record were public individuals in well publicized positions and that they were referred to in that capacity and, as a result, the disclosure of the names did not amount to an unreasonable invasion of their privacy. She further found that everything in a record identified as "responsive" to an access to information request is relevant to the request and that the entire record should be disclosed unless portions of the record fall within one of the limited exclusions set out in sections 13 to 25 of the Act because seemingly irrelevant information can provide context. She recommended the disclosure of additional information.

Review Report 20-214

Category of Review: Access to Information

Public Body Involved: Department of Environment and Natural Resources

Sections of the Act Applied: Section 9, Section 13, Section 15, Section 23

Outcome: Eight of 124 recommendations not accepted

The Applicant requested information in relation to the change of Directors for the Independent Environmental Monitoring Agency for a stated period of time. A large number of records were disclosed but with many redactions. The Applicant also felt that not all responsive records had been provided.

The IPC reviewed each record and made 124 recommendations for the disclosure of addtional information.

Review Report 20-215

Category of Review: Privacy Breach Complaint

Public Body Involved: Department of Industry, Tourism and Investment

Sections of the Act Applied: Section 43, Section 48

Outcome: No response received

The Complainant alleged that in the course of responding to an access request, the ATIPP Coordinator revealed the Complainant as the Applicant, resulting in a breach of his privacy. The Complainant further alleged that his personal information was then inappropriately used by his supervisor in an internal proceeding in an attempt to discredit him.

While conceding that the ATIPP Coordinator made an error in revealing the identity of the Complainant as the Applicant in an access to information request, the department pointed out that it is information that would have been assumed by those conducting the searches for responsive records because it was a request for the Applicant's own personal information which required the disclosure of the name. They further conceded that because the information had been inappropriately used by the public body, the subsequent disclosure of the information by the Complainant's supervisor was also unauthorized.

The IPC found that there had been a breach of the Complainant's privacy in both instances and recommended that the Department review and update its policies to reflect the pending coming into force of Bill 29 - *An Act to Amend the Access to Information and Protection of Privacy Act*. She also recommended updated and ongoing training for ATIPP Coordinators in the Department. Finally, she recommended that the Department develop a policy or procedure to provide an appropriate process for employees to report apparent privacy breaches to appropriate officials.

Review Report 20-216

Category of Review: Access to Information

Public Body Involved: Department of Finance

Sections of the Act Applied: Section 14(1)(a), Section 14(1)(b), Section 23

Outcome: Recommendations accepted

The Applicant sought records in relation to a labour dispute involving himself. The Department provided a large package of responsive records, but there was significant information redacted under sections 14 and 23 of the Act.

The IPC reviewed all the responsive records and recommended the disclosure of additional information. With respect to section 23 (unreasonable invasion of third party privacy) she pointed out that information about employees in carrying out their employment responsibilities was not protected from

disclosure. She further found that for records containing only factual information or a statement about a decision made, section 14 did not apply as there was no active advice, recommendations, analysis or similar information involved in these records.

Review Report 20-217

Category of Review: Access to Information

Public Body Involved: Northwest Territories Housing Corporation

Sections of the Act Applied: Section 1, Section 2, Section 3, Section 6, Section 7, Section 8, Section 33, Section 59(2)

Outcome: Redacted records disclosed

Recommendation to prosecute not accepted

On October 15th, 2019 the Applicant made a request for information in which he or his position was discussed among a number of named individuals. When NTHC failed to respond by November 24th, the Applicant asked the OIPC for assistance. The IPC encouraged the Applicant to follow up directly with the NTHC before raising it to the level of a review. On December 10th, having still not received a response, the Applicant filed a formal Request for Review on the basis of a deemed refusal pursuant to section 8. The IPC wrote to the NTHC and gave them the opportunity to respond to the Applicant by January 6th to avoid a review. When no response was provided, the IPC requested NTHC to provide copies of all responsive records and submissions by January 20th. Follow up letters were sent on January 15th, February 5th and February 18th. No response was received.

The IPC found that the onus was on the public body to establish that an Applicant had no right to access to a record and, because the NTHC had not responded in any way, either to the Applicant or to the IPC, she recommended the disclosure of all records except any record subject to an applicable mandatory exception. She further recommended that the President of the NTHC delegate his authority to respond to her recommendations to the Minister responsible for the NTHC and that the President and the ATIPP Coordinator be prosecuted under section 59(2) of the Act.

Review Report 20-218

Category of Review: Access to Information

Public Body Involved: Northwest Territories Housing Corporation

Sections of the Act Applied: Section 1, Section 2, Section 3, Section 6, Section 7, Section 8, Section 33, Section 59(2)

Outcome: Redacted Records Disclosed

Recommendation to Prosecute not accepted

The Applicant made a request for information from the NTHC on July 16th, 2019. Because the NTHC failed to respond to the Request for Information by August 27th, the Applicant requested the OIPC to review the matter on the basis of a deemed refusal. On September 6th, 2019, the IPC wrote to the NTHC and in an attempt to avoid the lengthy formal review process, gave them the opportunity to respond to the Applicant's Request for Information by September 13th. On September 13th, the NTHC confirmed that they had sent the responsive records to the Applicant, which he confirmed as received on October 10th. On October 13th, the Applicant sought a review of the response received on the basis that NTHC had not fully complied with the request. On November 25th, the IPC requested submissions from the NTHC to be provided by January 2nd. Follow up letters were written on January 14th, February 4th and February 18th, on which date the NTHC was

informed that the IPC would be proceeding with the review based on the Applicant's submissions only. NTHC failed to respond in any way and on March 10th, the IPC issued her Review Report, recommending the disclosure of all responsive records subject only to information subject to a mandatory exception under the Act. She further recommended that the President of the NTHC delegate his authority to respond to the Review Report to the Minister Responsible, and that the President and the ATIPP Coordinator for the NTHC be prosecuted pursuant to section 59.

Review Report 20-219

Category of Review: Access to Information

Public Body Involved: Department of Finance

Sections of the Act Applied: Section 14(1)(a), Section 22, Section 23

Outcome: Recommendations mostly accepted

The Applicant made a request for records related to his own personal information held by the Department of Finance. More specifically, the Applicant requested records about himself related to a labour dispute. He received a large volume of records. However, a significant number of the records were withheld or partially withheld pursuant to sections 14(1)(a), 22 and 23(1).

The IPC reviewed the law applicable to each of these exceptions and analyzed each of the items redacted or withheld. She determined that much of the information withheld pursuant to section 14(1)(a), which gives public bodies the discretion to withhold information which could be reasonably expected to reveal advice, proposals, recommendations, analyses or policy options, did not meet the necessary criteria for the exception and recommended further disclosures. She found that the disclosure of a name and associated business address will not, in most instances, amount to an unreasonable invasion of privacy pursuant to section 23.

Review Report 20-220

Category of Review: Access to Information - Delay

Public Body Involved: Department of Finance

Sections of the Act Applied: Section 7, Section 8, Section 11,

Outcome: Recommendations accepted

The Applicant made a request for information on February 21st, 2019. The request was acknowledged by the Department on February 25th. In an undated letter, received by the Applicant on March 27th, the public body purported to extend the time for responding to April 26th pursuant to section 11 of the Act because the request involved a "large number of records". On April 29th, the Department provided the Applicant with one set of records and told the Applicant the second set would be provided by May 17th. The Applicant objected to the second extension and on May 2nd asked the OPIC to review the matter. The second set of records was provided to the Applicant on May 29th.

The IPC found that the public body failed to meet legislated time frames under the Act three times during the course of responding to the Applicant. She further found that when taking an extension pursuant to section 11(1)(b) of the Act (where there are a "large number of records" and meeting the time limit would unreasonably interfere with the operations of the public body) the public body must provide some evidence not only that there are a large number of records, but also that complying with the time frame would interfere with the operations of the public body. She pointed out that this does not mean it would tax the ATIPP Coordinator but that the operations of the public body would be affected overall.

Further, while the public body relied on section 11(1)(b) in its correspondence with the Applicant extending the time, when explaining the delay to the IPC they argued, instead, that there was a need to review several records internally (not a reason for extension under the Act) and this was in fact the reason for the delay. The public body also indicated that the delay was, in part, due to workloads within the department and lengthy review processes, which are also not reasons for not meeting the time frame for responding.

The IPC recommended that the Department of Finance ensure that it has a sufficiently trained and dedicated cohort of staff to address access to information requests and that they create internal guidelines and procedures to ensure that, even where there are a large number of records, they can respond effectively and efficiently and within the thirty day time frame.

Review Report 20-221

Category of Review: Privacy Breach Complaint

Public Body Involved: Department of Industry, Tourism and Investment

Sections of the Act Applied: Section 1, Section 24

Outcome: No recommendations made

The Complainant alleged that the Department of ITI had disclosed information about its financial situation to potential buyers of his business resulting in him being unable to sell the business for top dollar. He alleged that an employee at ITI, who had provided the company with financial assistance, had advised potential buyers that the company was going to be declaring bankruptcy and that they would be better to wait until that happened because the price of the business would then fall. ITI denied the allegation, stating that it was in the public body's best interests, as well as the business owner's, that the business attract the highest price possible.

The IPC could find no evidence that the ITI employee had disclosed any business information about the Complainant's business and made no recommendations.

Review Report 20-222

Category of Review: Access to Information

Public Body Involved: Department of Health and Social Services

Sections of the Act Applied: Section 1, Section 5, Section 13(1), Section 14(1), section 23

Outcome: No response received

The Applicant made a request to the Department for information about discussions surrounding plans or proposals to develop a managed alcohol program in the Northwest Territories over a stated time frame.

The Department identified 38 pages of responsive records which were provided to the Applicant, but a number of the records were withheld in whole or in part pursuant to sections 13 (cabinet confidences), 14 (advice to officials) and 23 (unreasonable invasion of privacy).

The IPC found that the information withheld as a cabinet confidence did not meet the criteria for the exception and recommended it be disclosed. She recommended the disclosure of additional information under both section 14 and 23.

HEALTH INFORMATION ACT

Twelve Review Reports were issued pursuant to the *Health Information Act*.

Review Report 19-HIA 12

Category of Review: Privacy Breach Complaint

Custodian Involved: Hay River Health and Social Services Authority

Sections of the Act Applied: Section 10, Section 14, Section 16, Section 85

Outcome: Recommendations accepted

The Complainant attended an appointment at the clinic in Hay River for the purpose of having pictures taken of a skin condition so that they could be sent to a specialist. In previous appointments of a similar nature, either an RN or a physician had taken the pictures. On this occasion a clinic assistant (CA) was tasked with taking the pictures. The client felt that having someone other than a medically trained individual taking the pictures was a breach of his privacy, particularly as the area to be photographed was an area of the body that would be considered sensitive. The Complainant voiced his concerns and the CA offered to have a nurse take the pictures, an offer the Complainant declined in the interest of time.

The IPC found that there was no breach of the Complainant's privacy. The Complainant, having been given a choice to re-book the appointment to a time when the RN or physician was available, consented to proceeding with the CA taking the photos.

Recommendations were made with respect to the custodian's compliance with the Mandatory Training Policy, with respect to communications with clients and with respect to ensuring appropriate consent.

Review Report 19-HIA 13

Category of Review: Privacy Breach Complaint

Custodian Involved: NTHSSA - Yellowknife Region

Sections of the Act Applied: Section 8, Section 10, Section 11

Outcome: Recommendations partially accepted

The Complainant was an employee of the NTHSSA who had several concerns about the processes and procedures in place resulting in what he considered to be a risk to privacy. He had expressed his concerns with his supervisors but had received no satisfactory response. These concerns included:

- While access to the electronic medical record (EMR) was controlled by "roles", everyone having even the base access level has access to the "encounter record" which lists, among other things, all of the reasons a client has accessed an appointment and often reveals other sensitive personal health information (PHI) such as mental health diagnosis, participation in a methadone program, cancer treatments and abortions. He felt that too much information was made available to too many employees with no need to know;
- No routine auditing was done to dissuade inappropriate access to individual client files;
- NTHSSA still uses a "circle of care" concept for the provision of health services allowing access to a client's files by anyone within a client's "circle of care" but without any definition of what that "circle of care" is or any consent from the client;
- The EMR does not have the ability to hide certain PHI from specific EMR users so the patient has no ability to prevent access by specified employees of the health system, for

example, a neighbor or an ex-spouse. Furthermore, clients are not told that they have the right to control who has access to their medical files;

- Notes from psychiatric nurses and psychiatrists with the out-patient program are stored on the EMR in a screen available to all EMR users;
- Practitioners do not understand "implied consent" as it relates to the collection, use and disclosure of personal health information;
- Health care professionals continue to use unencrypted emails to transfer PHI
- Those granted access at a particular level in the EMR then has that level of access for all NWT residents within the NTHSSA system, regardless of where they reside.

The IPC reviewed each of the issues raised by the Complainant and found that many of the concerns expressed were well founded. She made 13 recommendations to improve general privacy policies and procedures within NTHSSA, including:

- that NTHSSA review all of its public education materials to remove reference to "circle of care" and to discontinue the use of the term within the organization as this is not a concept recognized in the HIA
- that NTHSSA take immediate steps to give honest and true effect to sections 22 and 24 of the *Health Information Act*, whether by way of an electronic solution (masking) or some other consistent and effective process;
- that NTHSSA develop and enforce policies which direct all of its employees and agents to use the most privacy protective tools available to them when communicating information about patients, to include a hierarchy of appropriate means of communication.
- that NTHSSA create and disseminate a public education campaign to educate the public about how the *Health Information Act* affects the patient, and outlines the patient's rights including, most importantly, the right to place conditions on how personal health information can be collected, used and disclosed and the right to withdraw consent to the collection, use and disclosure of personal health information.

Review Report 19-HIA 14

Category of Review: Breach Notification

Custodian Involved: Department of Health and Social Services - Public Health

Sections of the Act Applied: Section 28(2), Section 85, Section 87(b), Regulation 15

Outcome: Recommendations largely accepted, but many only "in principal"

The Department of Health and Social Services gave the OIPC notice that an unencrypted laptop containing personal health information of almost 40,000 NWT residents had been stolen from an employee's vehicle in Ottawa.

The IPC reviewed the incident and described the information on the laptop and all of the steps taken by the Department of Health in the wake of the theft. She expressed concern about the Department's interpretation of some of the evidence and some of the sections of the *Health Information Act*, their apparent lack of knowledge of their own policies as well as of the logic of some of the conclusions in relation to the cause of the breach as contained in the Department's internal investigation.

She made a number of findings, including:

- the theft of the laptop constituted a breach of privacy under the Act, and that this would have been the case even if the device had been encrypted.

- the Department's focus on whether or not the theft might result in identity fraud or financial loss was misguided and that the question that the department should have been asking was not whether the risk of harm amounted to a privacy breach, but whether as a result of the privacy breach (theft) there was a risk of harm to the individuals whose privacy was breached.
- the Department failed to acknowledge that one of the most significant effects of the breach in this case is the risk that the people of the Northwest Territories will lose confidence in the ability of the Department of Health and Social Services to adequately protect their most sensitive personal health information, which in turn, negatively impacts on the effectiveness of the health system and the health of residents of the Northwest Territories as a whole.
- the information on the laptop should never have been downloaded to the laptop and removed from the safety of the GNWT server system. N otwithstanding existing policies, procedures and safeguards, the employee's supervisor authorized and sanctioned the employee's practice of downloading sensitive personal health information onto a mobile device in direct contravention of all of those policies, procedures and safeguards.
- TSC also failed to follow its own policies by failing to encrypt the laptop before releasing it to the Department and by failing to follow its own "evergreening" policies and that these failures increased the seriousness of the breach.

The IPC made 15 recommendations arising out of this breach, which included the following:

- that all remaining Lenovo Helix laptops still in use be retired;
- that the Department develop a detailed policy to address circumstances in which records containing PHI can be downloaded to a mobile device;
- that steps be taken to ensure that Population Health has sufficient human resources to do their work without having to take the work out of the office;
- that the Deputy Minister take action to ensure compliance with privacy policies issued under the HIA;
- that Population Health immediately cease the practice of downloading records containing PHI to mobile devices for the purpose of working remotely except in exigent or emergent circumstances;
- that a thorough privacy audit be conducted by an independent expert in the fields of both population health and health privacy to assess the manner in which information is gathered by Population Health, including the kinds of information collected, the justification for each data element, the means of collection, and the safeguards in place to protect the information.

Review Report 19-HIA 15

Category of Review: Privacy Breach Complaint

Custodian Involved: NTHSSA - Stanton Territorial Hospital

Sections of the Act Applied: Section 44, Section 84

Outcome: Recommendations accepted

The Complainant asked the OIPC to investigate whether his personal health information had been inappropriately disclosed to his employer or his employer's legal counsel. He was a patient at the Stanton Territorial Hospital (STH) as a result of illness and complications arising out of that

illness. He lived in a community other than Yellowknife and returned to his community when discharged but was unable to return to work for a period of time. His employer asked him to resign or retire and the matter ended up in the courts in the form of a claim for wrongful dismissal. During the course of discovery in that court action, counsel for the employer produced several pages of detailed medical records in relation to the Complainant's stay at the STH and it appeared from markings on the papers that the documents had been faxed from STH but it is unclear where they had been faxed to.

STH indicated that it is their practice to send a medical information package to the health centre in the patient's home community for the purpose of continuing care when the patient is discharged and that it appeared that the records obtained by the employer's counsel were these records. Because the patient's discharge had happened more than two years earlier, however, the hospital no longer had the fax logs associated with the transfer as these are kept for only one year. The IPC found that there was no evidence that the breach in this case was perpetrated by the STH and that it was more likely that the breach originated in the Complainant's home community. However, the IPC made recommendations to improve privacy protections for patients. These included ensuring that a record of all disclosures without the express consent of the patient be maintained and that the STH include a step in their discharge protocol to verify with patients that relevant records will be sent to the health centre in the patient's home community.

That said, best practices would include a notification to the patient, where possible, that his/her personal health information is being transferred to health care providers in his/her home community. It seems to me that this is just common courtesy, quite apart from any legislated requirement.

Review Report 19-HIA 15

Review Report 19-HIA 16

Category of Review: Breach Notification

Custodian Involved: NTHSSA - Yellowknife Region

Sections of the Act Applied: Section 17, Section 14, Section 15

Outcome: Recommendation accepted and transferred to Department of Health and Social Services for implementation

A mental health counselor received a referral for a client under the age of 16. The counsellor knew the client's family and knew that at least one of his parents was an employee of the GNWT. The counsellor felt that since the parent was a GNWT employee, the client could be supported by the Employee Assistance Program (EAP) and approached the parent to provide information about that program, revealing the client's referral in doing so. As a result of the breach, NTHSSA had taken proactive steps, including developing an SOP on the issue of "consent to treatment". The IPC's review focused on policies required to deal with the issue of obtaining consent to the collection, use and disclosure of personal health information (as opposed to consent for treatment, which is different) for minors and, in particular, for mature minors.

During the course of the review, it was revealed that there were no comprehensive policies in place on the issue of consent, whether for the purposes of treatment and care, or in relation to the collection, use and disclosure of personal health information.

The IPC recommended that NTHSSA develop formal guidelines with respect to obtaining valid consent for the collection, use and disclosure of personal health information, including provisions in relation to obtaining such consent from mature minors.

Review Report 19-HIA 17

Category of Review: Breach Notification

Custodian Involved: NTHSSA - Yellowknife Region

Sections of the Act Applied: Section 8, Section 85, Regulation 13, Section 88, Regulation 14, Section 87, Regulation 15

Outcome: Recommendations accepted except for four which were forwarded to the Department of Health and Social Services for consideration/implementation

This review report addressed a common theme in several breach notifications received over the course of approximately 6 months. In each of these cases, a breach of privacy resulted from the failure of an employee to verify the identity of the patient using two person-specific identifiers, such as a name and birthdate, or a name and a health card number.

In one case, an invoice for health services was given to the wrong client. Three other cases involved prescriptions being created in the wrong name or being given to the wrong patient. In the last incident a client was misidentified throughout an entire clinic visit, involving no less than four staff/client interactions, and culminating with the issuance of a prescription containing the name, date of birth, personal health care number and contact information of another individual.

The IPC found in each case that the cause of the breach was the failure of NTHSSA staff to follow protocol with respect to the use of two person-specific identifiers to confirm the identity of the client. She found that while the custodian had taken some measures required under HIA section 85 to protect the confidentiality of personal health information by having a policy in place and by way of staff awareness efforts, it failed to apply and/or fully adhere to existing measures, and in some cases the measures in place were lacking which resulted, in each case, in the unauthorized use and disclosure of personal health information. The IPC reviewed existing policies, including the Privacy Breach Policy, the Mandatory Privacy Training Policy, and the Client/Identifiers Policy.

The IPC made recommendations for revisions to the Mandatory Privacy Training policy, the Privacy Breach Policy and the Client/Patient Identifiers Policy. Further, she recommended the development of clear, step-by-step directions to staff on how to apply the patient identifier protocol. Recommendations were also made with respect to ensuring compliance with the Mandatory Privacy Training policy and that privacy training require a measure or test to demonstrate comprehension of training received on the part of each staff person

Review Report 19-HIA 18

Category of Review: Breach of Privacy Complaint – Non-Compliance with Conditions Placed

Public Body Involved:
NTHSSA - Beaufort-Delta Region

Sections of the Act Applied: Section 22, Section 87, Section 192, Regulation 14

Outcome: Recommendation to comply with complainant's consent condition as required by section 22(3) not accepted

Recommendation to comply with Section 11 of the HIA not accepted

Remaining recommendations accepted

The Complainant, an employee of NTHSSA in the Beaufort-Delta Region, had some health issues that he did not want his co-workers to know about, particularly those he worked with directly. He attempted to institute an appropriate condition on the use/disclosure of his personal health information on his chart pursuant to section 22 of the HIA. The condition was not implemented as requested and, as a result, the Complainant expected that other NTHSSA staff had inappropriately accessed his medical record resulting in a breach of his privacy.

The IPC discussed section 22 of the HIA which outlines the right of the individual to place conditions on how their personal health information may be collected, used and disclosed. Despite making the request a number of times over the course of at least two years, NTHSSA failed to implement the condition on the Complainant's electronic health record, largely, it appeared, because they could not find a way to do so that seemed satisfactory to management.

The IPC found that information in NTHSSA's *Health Information Act* Guide which stated that "if the custodian's system does not have the technical capacity to mask the information or if it is considered not within professional standards to mask that information, the custodian will not be required to meet the condition" was wrong in law as there was nothing in the HIA which supported this statement.

The IPC's recommendations included the following:

- that NTHSSA take immediate steps to comply with the Applicant's consent conditions and provide the Applicant and the OICP with confirmation of what steps had been taken
- that NTHSSA take immediate steps to ensure that its electronic health records system includes the ability to mask PHI and/or to prevent access by one or more discrete individuals so as to allow compliance with section 22 of the *Health Information Act*.
- that the HIA Guide be amended to remove the erroneous statement contained in that document which suggests that if the custodian does not have the technical ability to comply with a condition, the custodian is not required to do so and so that it instead reflects the law which requires a public health information custodian to "take reasonable steps" to comply with the condition.
- that the NTHSSA make its privacy policies, as reflected by the Ministerial Directive issued by the Minister of Health and Social Services in March, 2017, available on its website in a manner that makes these records easy to find and accessed by the public.
- that the NTHSSA take immediate steps to conduct a privacy breach investigation into the breaches alleged by the Applicant in accordance with its Privacy Breach Policy and provide a copy of that report to the Applicant on or before March 31st, 2020.

Review Report 20-HIA 19

Category of Review: Breach Notification

Custodian Involved: Hay River Health and Social Services Authority

Sections of the Act Applied: Section 153, Section 154, Section 186, Section 38 Regulation 14,

Outcome: Recommendations acknowledged but not clearly accepted

A client of HRHSSA requested his own personal health information. When he received the package, it contained one document containing the personal health information about another individual who had the same first and last names, but a different date of birth and who was from a different community.

When investigating how this happened, it appears that the error occurred when a clerk with Northwest Territories Health and Social Services recorded a medical travel form into the Hay River client's chart in error, having failed to compare at least two patient identifiers.

As a preliminary matter, the IPC commented on the failure of HRHSSA to cooperate with the investigation by her office. She found it necessary to write four letters requesting a response to her inquiries and then received only a very unsatisfactory and brief summary of events. Another two letters from the IPC were required before the HRHSSA provided necessary context and responses to questions. No final breach report as required by the Privacy Breach Policy was produced.

The IPC found that there had been two breaches in this case. The first was when the travel information for one client was placed on another client's file. The second was when the HRHSSA failed to properly review the information disclosed to the client to ensure it was accurate before releasing it.

In this case, HRHSSA took the position that the initial error was not made by their employee. The IPC found that because of the integrated nature of the EMR, there was an obligation to coordinate a response to a breach such as this where one custodian entered incorrect information into the chart of another custodian's patient. The IPC discussed accountability for the content on the shared, integrated EMR system and the need to ensure appropriate oversight for all users.

Several recommendations were made, including:

- that the persons responsible for dealing with privacy breaches at HRHSSA receive appropriate training in relation to applicable privacy laws and the organization's responsibilities in responding to breaches
- that HRHSSA work with the Department of Health and Social Services as well as the other health information custodians currently using the Wolf EMR system to outline a clear statement as to the respective responsibilities of all parties (users, owners, managers), including who is ultimately responsible and accountable for ensuring accuracy and management of the EMR.

Review Report 20-HIA 20

Category of Review: Breach Notification
Custodian Involved:
NTHSSA - Yellowknife Region

Sections of the Act Applied: Section 87, Regulation 14

Outcome: Recommendations accepted

The custodian in this case reported to the OIPC that a USB device containing a client's MRI of a head and neck injury had been lost. The USB had been provided by the client with the intention that it be added to his chart. The employee who received the USB device did not immediately take

it to his supervisor for processing, instead leaving it on his desk in a shared office space and when he came back to retrieve it, it could not be found.

The IPC reviewed an 'Administrative Directive' entitled "Encrypted USB Storage Devices, Use of". This was a policy put into place by the Yellowknife Health and Social Services Authority before the amalgamation of all Northwest Territories' Health Authorities into one entity. The content of that policy, however, did not address the situation in which a client provides a USB device, but only with the internal use of such devices. She also reviewed the custodian's response to the breach.

Several recommendations were made, including

- that privacy breach investigations be investigated in a timely manner (barring special circumstances, such investigations should be completed within 3 months)
- that steps be taken to ensure that NTHSSA complies with its Mandatory Privacy Training Policy
- that all privacy policies, SOPs and Administrative Directives be posted on NTHSSA's website for easy access by employees and the public
- that NTHSSA develop a policy to address situations in which clients wish to add digital information to their health records

Review Report 20-HIA 21

Category of Review: Breach Notification

Public Body Involved: NTHSSA - Child and Family Services Division

Sections of the Act Applied: Section 39, Section 87, Regulation 14

Outcome: Recommendations accepted

The Director gave the OIPC notice of a breach which occurred when an employee of CFS inadvertently emailed a *Mental Health Act* form containing sensitive personal health information about a client to an NTHSSA employee in Fort Smith instead of to the intended recipient in Yellowknife. The error happened because the intended recipient had the same first name as the employee whose name was inserted in the "To:" field and the sender did not pay adequate attention. The form was sent as an attachment to the email and was not password protected or encrypted.

The IPC found that emailing this document to the wrong person constituted an unauthorized disclosure under the HIA. The IPC reviewed the Health and Social Services Electronically Stored and Transferred Information Policy, which includes a direction that whenever personal, personal health and confidential information is electronically transferred it must be appropriately encrypted and/or password protected. She observed that in her experience this was a policy more often ignored than followed throughout the NTHSSA system.

The recommendations made included:

- that the NTHSSA post its Health and Social Services Electronically Stored and Transferred Information Policy on its website so that the public and staff are aware of its existence and it can be readily accessed;

- that the NTHSSA take immediate steps to ensure compliance with the Electronically Stored and Transferred Information Policy whenever documents containing personal health information are being transferred from one person to another, and in particular that the requirement for encryption or password protection be enforced.
- that the Mandatory Privacy Training Policy be extended to employees in the "social services" mandate of NTHSSA;
- that NTHSSA create a number of educational modules in relation to privacy best practices in the health and social services system focusing on various discrete topics and that these modules be added to, multiplied and updated from time to time to reflect lessons learned and new developments.

Review Report 20-HIA 22

Category of Review: Breach Notification

Custodian Involved: NTHSSA - Dehcho Region

Sections of the Act Applied: Section 85, Section 86

Outcome: Recommendation to prosecute complainant referred to Department of Justice

Recommendation to share report with all departments not accepted

All Remaining Recommendations Accepted

The OPIC received notice from NTHSSA that a resident in Fort Simpson had allegedly found a box full of files in the salvage area of the Fort Simpson dump and had provided a local CBC reporter with access to the records. The files contained dated mental health and addictions information about a large number of people.

This was a very complex review, and the IPC made a number of findings, including:

- while impossible to determine exactly where the found files originated, it is probable that they were created either in Fort Simpson by the LKFN under contract with the GNWT to provide counselling services between the late 1980s until the early 2000s, or on the Hay River Reserve in connection with a similar arrangement
- either way, it is probable that the box of files had been stored in the basement of the SISH building in Fort Simpson for some years
- the security of the storage area in the basement of the SISH building was, at best, weak and tended more to non-existent at the time of the breach
- while impossible to confirm how the resident of Fort Simpson came to be in possession of the files, it is possible that they were, in fact, found in the dump. It is also possible that the box of files was taken from the SISH during one of several "clean out" events at that facility in the summer and fall of 2018;
- based on the history of health and social services delivery in the Northwest Territories, the records in question were, at the time of the breach owned by the NTHSSA, and NTHSSA had custody and control of the records at the relevant time
- however the Fort Simpson resident came to be in the possession of the records, his possession constituted an unauthorized disclosure of personal health information under the HIA
- there were very few policies and procedures in place in the Dehcho Region (or any other region) in relation to the management of files in storage and no effective policies with respect to the retention and destruction of records

The following were among the 15 recommendations made:

- that there be a full inventory of all stored materials in the custody or control of the NTHSSA
- that immediate steps be taken to assess the current administrative, physical and technological safeguards in place for the protection of personal health information at the SISH facility generally
- that COOs and senior managers of all regions complete and verify successful completion of all available privacy training modules;
- that urgent steps be taken to develop or actively adopt system wide policies and SOPs as require by section 8 of the HIA in relation to retention and destruction of records containing personal health information and the general management of inactive files;
- that the Mandatory Training Policy be centrally monitored and resources necessary be made available for enforcement, with a means to test understanding of training received, and that responsibility for monitoring and enforcement of this policy be delegated to a specific division of NTHSSA, with immediate and clear consequences for failure on the part of employees to comply, including the removal of access to medical records
- that consideration be given to prosecuting the Fort Simpson resident who found these records under section 185 of the *Health Information Act* so as to send a clear message to the public that it is not appropriate to disclose found personal health information to the press or to the public, regardless of the circumstances
- that steps be taken internally to address the failings of NTHSSA as the health information custodian, and of the NTHSSA-Dehcho Region, represented by Dehcho Region leadership, to provide adequate protection to the personal health information in their organization

Review Report 20-HIA 23

Category of Review: Correction to Personal Health Information

Custodian Involved: Hay River Health and Social Services Authority

Sections of the Act Applied: Section 125(a) and (b), Section 119, Section 120, Section 126, Section 142, Section 14, Section 15

Outcome: Recommendations agreed to "in principal"

The Applicant sought and received access to his personal health records for a five year period. When reviewing those records he discovered speculative statements recorded into his chart which appeared to have been subsequently used to make decisions about his treatment. He also objected to several of the opinions, comments and facts recorded as well as to the account of some events found in the records.

The Applicant made a request to correct or expunge a number of entries. The custodian agreed to remove reference to other members of the Applicant's family from the records but declined to make other corrections requested.

The main focus of the requested corrections were around an early entry in which a community third party not involved in the Applicant's direct care provided information to the custodian which was, in turn, recorded on his chart. This information alleged a suspected association by the Applicant with an particular group. There was no evidence to support the supposition and the

information amounted to nothing more than gossip or hearsay. It was clear, however, from subsequent notations on the file that, even years later, this old hearsay was being referred to and brought forward by subsequent locum physicians to make decisions about the patient's current treatment and care. The IPC found that the collection of the information from a third party source was not an authorized collection. The IPC further found that there were a number of other entries that constituted the legitimate professional opinion of the health care provider and that such opinions were properly a part of the patient's file.

The IPC recommended that the information obtained from an unverified third party source be removed from the record, as well as any subsequent references to that information. She also made comments on a consent form being relied on by the HRHSSA as consent to the collection from and disclosure to third party service providers and recommended changes to that form.

PRIVACY IS ESSENTIAL

Grounded in a man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy or constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.

Justice G. LaForest
R v. Dyment [1988] 2 SCR 417, SCC

TRENDS AND ISSUES MOVING FORWARD

The next few years for the Office of the Information and Privacy Commissioner will be a time of change and adjustments, with new legislation coming into force and a new Information and Privacy Commissioner taking the helm. All of this is happening in the unprecedented circumstances presented by COVID 19, which will have lasting effects on the way both government and businesses work.

Preparing Municipalities

The new legislation lays the groundwork to include municipal and community governments under the Act. Before this can happen, all municipal governments will need to be ready to meet the obligations imposed by the legislation. This will include not only education and training, but also an upgrading of information management systems which will allow municipalities to search for and find public records effectively. Resources should be set aside and investments made as soon as practically possible to begin this process so that the costs of implementation of the access provisions of the Act are not immediately overwhelming. In the meantime, the privacy provisions of the Act can be implemented with little additional cost but for education and training and I would recommend that this training begin as soon as possible.

COVID 19 Response

COVID 19 created an urgent need to find ways to work and provide services from outside the confines of the traditional office space. As a result, many new technologies have been implemented without adequate vetting or privacy impact assessments having been done. Once things have settled out a bit it will be necessary to retrace steps to fully and properly assess the privacy impacts of these new approaches and technologies, especially in those circumstances in which there is a determination that the continued use of these work-around solutions may be effective on a permanent basis. There has never been a greater threat to privacy than now and there must be a clear commitment to continuing to make privacy a priority regardless of perceived benefits of these new approaches. Long term impacts must also be considered.

The pandemic has also resulted in the collection of huge amounts of personal information. Most public bodies, including health care facilities, now collect the personal information of every person entering a facility. Anyone who travels outside of the Northwest Territories must now provide significant amounts of personal information in order to qualify to return to their own home. Names and addresses and telephone contact information is now being required in circumstances in which one would never have dreamed of providing such information only a few short months ago. There is a legitimate need for the collection of much of this information, but there seems to be little guidance as to the retention and destruction of this information when it is no longer required for the purposes for which it was collected (i.e. contact tracing). While responding to and continuing to plan for the pandemic is important, it is equally as important that we continue to monitor the privacy impacts of the steps taken to address these issues so that we do not lose our constitutional and human right to determine how and by whom our personal information is collected, used and disclosed.

Training for ATIPP Staff

If one were to read all of the Review Reports issued over the past year, one of the most commonly recurring themes in terms of recommendations is that public bodies provide their ATIPP Coordinators with more and better training with respect to their roles as the gatekeepers within the departments on these issues. The position of ATIPP Coordinator is an important one and requires the ability and the authority to make decisions with respect to what is, and what is not, appropriate to disclose in the context of an access to information request, and who understands and has the ability to address privacy concerns raised. These positions are not entry level positions. They require expertise and training, a strong familiarity with records management and an understanding of the way in which the GNWT operates. The GNWT has lost a number of its most experienced ATIPP Coordinators over the last year and this is becoming obvious in the quality of responses to both Applicants and to this office. The importance of the role and the expertise required in an ATIPP officer needs to be recognized in the form of appropriate ratings for position evaluation and remuneration commensurate with the importance and expertise required. More ATIPP Coordinators should be encouraged and supported to take on-line training such as that offered by the University of Alberta's Faculty of Extension. ATIPP Coordinators should be encouraged to meet on a regular basis to discuss issues that have presented themselves and solutions applied. In short, more must be done to invest in, support and train these important employees.

Adequate Resources

Bill 29 –*An Act to Amend the Access to Information and Protection of Privacy Act* will bring a modernized and much improved approach to access and privacy in the Northwest Territories. It would be naïve, however, to think that these new provisions can be implemented with no additional resources being dedicated to compliance. If the last year has proven anything, it is that access and privacy issues continue to grow in prominence and importance. I predict that the coming years will be increasingly busy for the Office of the Information and Privacy Commissioner. Just as I have advocated for adequate resources be provided to public bodies, it is equally important that adequate staff and appropriate expertise be allocated to the OIPC to meet its obligations under the Acts and to meet the ever increasing demand for its services. With one new investigator having been approved for the 2020/2021 fiscal year, this will hopefully help to reduce the existing backlog and allow the new Information and Privacy Commissioner some breathing room. While this will give the office the human resources it needs to meet existing demand, it will not be nearly sufficient to meet the anticipated need once the new legislation comes into effect.

Privacy Impact Assessments

As noted above, this office has spent many hours reviewing privacy impact assessments provided by health information custodians as required pursuant to section 89 of the *Health Information Act*. Bill 29, *An Act to Amend the Access to Information and Protection of Privacy Act* will, when it comes into effect, also impose on all public bodies a similar requirement to conduct PIAs for new projects involving the collection, use or disclosure of personal information. PIAs are

important tools to help assess how a project will impact on privacy, to identify any privacy impacts contrary to law and to help in addressing those impacts as effectively as possible. The PIA is a living document, which should be continuously referred to and updated as necessary. A good PIA process will begin at the conceptual stage of any project to identify issues such as necessity, proportionality, effectiveness and minimal intrusion. It will be reviewed and updated during the development stage and address issues such as identifying the specific purpose for each data point collected, necessary consents, legislative compliance, safeguards, internal controls, training and operational responsibility. Once a project is complete, the PIA should continue to be used to test effectiveness and identify new impacts that might come to light over time. Done well, PIAs will ensure compliance with privacy legislation and avoid costly and time consuming attempts to address issues after the fact. They are an essential tool in the "Privacy by Design" concept which contemplates building privacy into new projects from the inception.

In light of the existing PIA obligations placed on health information custodians and the pending obligations in this regard which will come into effect with the amendments to the *Access to Information and Protection of Privacy Act*, I would strongly recommend that detailed policies and procedures be created to ensure that this tool is both understood and effectively used to measure the impacts of new programs, to include a requirement to engage the Office of the Information and Privacy Commissioner in identifying discrepancies in compliance. Further, the direction should include a requirement to engage the Office of the Information and Privacy Commissioner in the planning stages of projects rather than only after the project is implemented.

FINAL WORD

As I leave the position of Information and Privacy Commissioner for the Northwest Territories, I feel a sense of accomplishment and satisfaction. I am proud of the work that has been done by my office over the last twenty-four years to improve access and privacy for the people of the Northwest Territories. The job has had its challenges and frustrations, but that is the nature of the beast and nothing worth having comes without hard work and perseverance and sometimes even a little pain. I have become a strong advocate for the values espoused by the legislation over which I have had oversight. My hope is that I have left this office strong and ready for the next Information and Privacy Commissioner to be able to continue this important work supporting privacy and access to information rights.