

**Office of the Information  
And Privacy Commissioner of the  
Northwest Territories**

**ANNUAL REPORT  
2018/2019**







**OFFICE OF THE  
INFORMATION  
AND PRIVACY  
COMMISSIONER**  
NORTHWEST TERRITORIES

P.O. Box 382  
Yellowknife, NT  
X1A 2N3

August 10, 2019

The Hon. Jackson Lafferty  
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, 2018 to March 31st, 2019.

Yours very truly

Elaine Keenan Bengts  
Information and Privacy Commissioner  
Northwest Territories

/kb





## TABLE OF CONTENTS

<b>COMMISSIONER'S MESSAGE</b>	<b>3</b>
<b>FINANCIALS</b>	<b>7</b>
<b>ABOUT THE OFFICE</b>	<b>8</b>
Access to Information and Protection of Privacy Act	8
The Health Information Act	8
The Role of the Information and Privacy Commissioner	9
<b>THE YEAR IN REVIEW</b>	<b>11</b>
<i>Access to Information and Protection of Privacy Act</i>	11
<i>Health Information Act</i>	13
<b>REVIEW REPORTS</b>	<b>15</b>
<i>Access to Information and Protection of Privacy Act</i>	15
Review Report 18-178	15
Review Report 18-179	16
Review Report 18-180	17
Review Report 18-181	17
Review Report 18-183	19
Review Report 18-184	19
Review Report 18-185	20
Review Report 18-186	20
Review Report 18-187	21
Review Report 18-188	22
Review Report 18-189	23
Review Report 18-190	24



<b>Review Report 18-191</b>	<b>24</b>
<b>Review Report 18-192</b>	<b>25</b>
<b>Review Report 18-193</b>	<b>26</b>
<b>Review Report 18-194</b>	<b>26</b>
<b>Review Report 19-195</b>	<b>27</b>
<b><i>Health Information Act</i></b>	<b>28</b>
<b>Review Report 18-HIA04</b>	<b>28</b>
<b>Review Report 18-HIA05</b>	<b>29</b>
<b>Review Report 18-HIA06</b>	<b>30</b>
<b>Review Report 19-HIA07</b>	<b>31</b>
<b>Review Report 19-HIA08</b>	<b>32</b>
<b>Review Report 19-HIA09</b>	<b>33</b>
<b>Review Report 19-HIA10</b>	<b>34</b>
<b>TRENDS AND ISSUES MOVING FORWARD</b>	<b>36</b>
<b>Municipalities</b>	<b>36</b>
<b>Public Bodies</b>	<b>37</b>
<b>The Office of the Information and Privacy Commissioner</b>	<b>37</b>
<b>Review of Policies</b>	<b>38</b>
<b>The Continued Use of Fax Technology in the Health Sector</b>	<b>39</b>



## COMMISSIONER'S MESSAGE

As the fiscal year began, my office anticipated a busy year ahead and that anticipation was well rewarded. Alongside our work resolving privacy complaints and reviews of access to information matters, we provided advice to the legislature and government departments on policy and compliance issues and advice to government on new legislation, amendments and new programs.

Both access to information and protection of privacy issues continue to grow more complex and challenging with each passing year. Public bodies are faced with an ever-increasing demand for access to information. The transition to digital records is all but complete in most areas of government, and as demonstrated by the steadily rising rate of inquiries to my office, I see in increasing public interest in government activity. The public is far more demanding in terms of the kinds of information they expect to receive about government and its activities than it was only a few years ago. Democratic institutions around the world are being challenged to be more and more transparent. Public confidence in government is tied closely to the ability of government to provide that transparency. Residents of the Northwest Territories, too, have demonstrated an increasingly keen interest in what their government is doing to meet its various mandates.

Over the last two years, the privacy landscape has taken what the Information and Privacy Commissioner of British Columbia, Michael McEvoy, has described as “a tectonic shift” following sensational revelations about how Facebook and Cambridge Analytica gathered and used personal information to influence various campaigns. This, combined with hundreds of highly publicized privacy breaches impacting millions of individuals and thousands of less highly publicized breaches occurring almost daily have resulted in a much more privacy aware public. Surveys show that Canadians are more aware of privacy issues than ever before and more careful about their own privacy.

In most instances, the sharing of personal information with government agencies is not a choice. If we want health care or education, or if we need a driver's licence or social supports, we have no option but to provide public bodies with our personal information. If government does not live up to its obligations to keep that information private and secure, the inevitable result will be a loss of trust in all aspects of government. It is no longer good



enough for any government to pay lip service to privacy impacts – all public bodies must operate with a privacy mandate front and centre.

These obligations will come into sharper focus with the coming into force of Bill 29, *An Act to Amend the Access to Information and Protection of Privacy Act* which passed first and second reading in 2018. This Bill was the culmination of work begun in 2012 and represents the first comprehensive review of the Act since its coming into effect on December 31, 1996. It contains many exciting new initiatives, including provisions necessary for bringing NWT municipalities under the Act. As I write this report, the Bill has now had third reading and received royal assent, setting the stage for bringing the new provisions into effect, hopefully in the next few months. During the committee review stage, the Bill was revised significantly and the resulting amendments will bring many forward-thinking changes to the way in which our office operates and access and how privacy matters are handled in the Northwest Territories. Those changes include:

- a) replacing the “recommendation only” powers of the Information and Privacy Commissioner with the power to make binding and court enforceable orders;
- b) providing the groundwork to include municipalities under the Act;
- c) requiring public bodies to pro-actively disclose risks of significant harm to the environment or to the health or safety of the public when that disclosure is clearly in the public interest;
- d) requiring public bodies to notify the Information and Privacy Commissioner when there has been a material breach of the privacy of one or more individuals, and to notify those individuals where the breach creates a real risk of significant harm to the individual;
- e) requiring all public bodies to complete a Privacy Impact Assessment (PIA) during the development of a proposed enactment, system, project, program or service that involves the collect, use or disclosure of personal information and to submit the PIA to the Information and Privacy Commissioner for review and comment;
- f) reducing the time that the Information and Privacy Commissioner has to complete a review from 180 calendar days (about six months) to 90 business days (about four and a half months);
- g) requiring public bodies to request extensions of time in excess of 20 days from the Information and Privacy Commissioner when they are unable to respond to a request for information on time.





- h) giving the Information and Privacy Commissioner the additional mandate of providing public education about access and privacy matters.

These are significant and substantive changes that will change the landscape dramatically and my office is looking forward to implementation. The transition from “recommendations” to “orders” is particularly significant and will require public bodies to put far more thought into their submissions to the Information and Privacy Commissioner during the review process, and to do a much better job of articulating their rationale for exercising their discretion to deny access where that discretion is given. The change to order making power will also challenge my office to be clear, concise and particular in relation to the orders made and the review process will need to become more formal with definitive and enforced time limits for submissions.

The Northwest Territories will be the fifth Canadian jurisdiction in which the Information and Privacy Commissioner makes binding orders, joining British Columbia, Alberta, Ontario and Prince Edward Island. The Federal Access to Information Commissioner is also transitioning from recommendations to order power. This is a positive change which I believe makes a lot of sense in today’s digital world.

2018/2019 was another busy one for the office with breaches in the health sector consuming a good portion of our time, including two very high-profile breaches. The first of these involved a stolen laptop containing personal health information of nearly every resident of the Northwest Territories. The second was the discovery of dated records containing sensitive personal information and, in some cases, personal health information, allegedly found in the dump in Fort Simpson. In addition to these two very well publicized breaches, the number of both breach complaints and mandatory breach notifications under the *Health Information Act* continued to grow as is reflected in the number of Review Reports issued under that Act.

I was very happy to welcome Dylan Gray to the office as the Assistant Commissioner/ Investigator on March 1<sup>st</sup> of this year. Dylan was previously with the Department of Health and Social Services as a Senior Privacy Specialist and his knowledge of the health sector in particular will be put to very good use. This doubles the size of our investigative team to two and we are working hard to clear the growing backlog.



I must also acknowledge the critically important work of our Office Manager, Lee Phypers, who is always organized and forever cheerful. Her dedication and knowledge about the work we do is essential to the smooth running of the office.

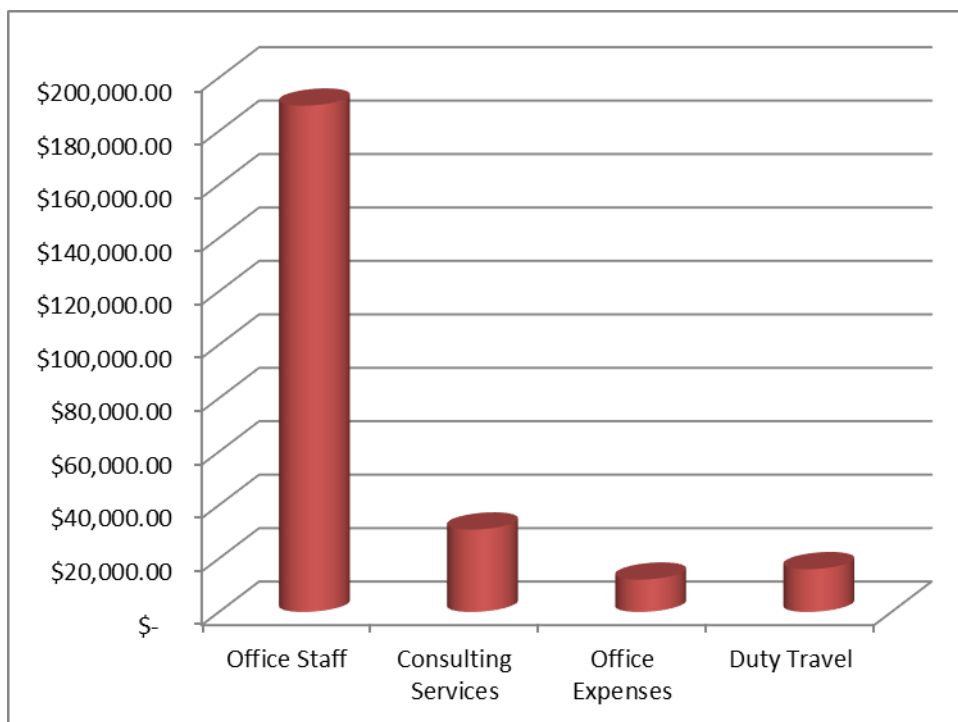
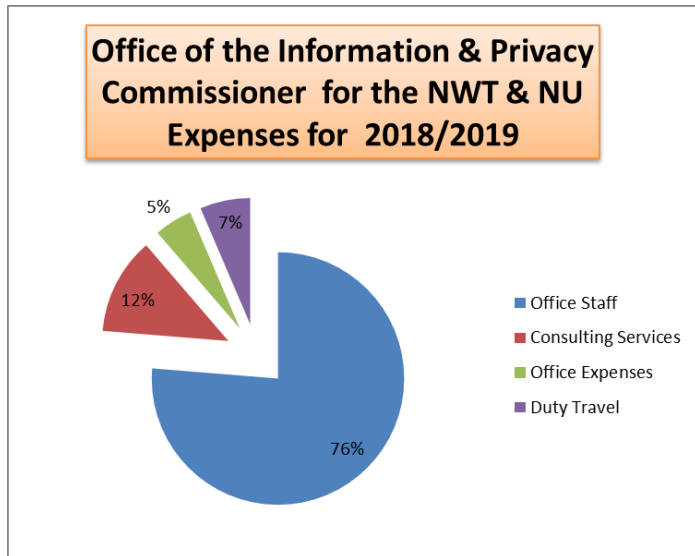


Participating on the Commissioner's Panel at the 2019 U of A Access and Privacy Conference



# FINANCIALS

The total (combined funds) spent to run the Office of the Information and Privacy Commissioner for the Northwest Territories and Nunavut for fiscal 2018/2019 was \$248,442.20. A detailed breakdown is outlined in the charts shown.





## ABOUT THE OFFICE

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 ATIPPA 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. 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, and 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 file.

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 improperly used or disclosed contrary to the Act, or is stolen, lost, altered or improperly destroyed. The Information and Privacy Commissioner may choose to do an investigation and prepare a report with appropriate recommendations in such circumstances.

## **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 request for information made to a public body or a health information custodian has been made but has not been answered to the satisfaction of the applicant, a Request for Review to the Office of the Information and Privacy Commissioner will trigger an independent review of the response. Similarly, if an individual has a privacy concern that has not been adequately addressed by a public body or a health information custodian, as the case may be, a request can be made to the Office of the Information and Privacy Commissioner to review the complaint.

The Information and Privacy Commissioner investigates the complaint 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. Neither public bodies nor health information custodians are currently required to accept the recommendations made, but the Information and Privacy Commissioner's reports are public records and the IPC is required to include in her Annual Report an indication of any recommendations made which are not 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 privacy impact assessments when requested to do so.

---

***Our access and privacy laws help ensure governments and organizations are held accountable for their actions. A transparent democracy gives us the information we need to participate actively, to criticize or support our government's decisions knowledgeably and to know we can trust our government to protect our personal information.***

Excerpt from 2018/2019 Annual Report of the Nova Scotia Information and Privacy



## THE YEAR IN REVIEW

The Office of the Information and Privacy Commissioner opened a total of 84 files in fiscal 2018-2019.

### *Access to Information and Protection of Privacy Act*

Fifty-five files were opened under the *Access to Information and Protection of Privacy Act* between April 1<sup>st</sup>, 2018 and March 31<sup>st</sup>, 2019. These can be broken down into a number of categories:

Requests for Review – Access to information	19
Requests for Review – Deemed refusal	8
Breach Notification from a public body	7
Requests for Review – Breach of privacy	6
Consultations/requests for comment	5
Miscellaneous	3
Requests for Review – Fees	2
Administrative	2
Breach Notification from a third party	1
Requests for Review – Extension of time	1
Request for Review – Third party consultation	1

These numbers indicate that once again by far the largest number of files opened related to requests for the Information and Privacy Commissioner to review responses received to access to information requests. There was a significant increase in the number of review requests pertaining to a failure by public bodies to respond to a request for information within 30 days, as required by the Act (deemed refusal). Most of these were resolved





without the need for a formal review, but it does indicate that there may be capacity issue developing in some public bodies.

I was pleased, this year, to be able to work with the City of Yellowknife in assessing the privacy impacts of their entry into Infrastructure Canada's Smart Cities Challenge. The City was a finalist in the five million dollar category and in their final submissions were required to assess any privacy impact that their project might need to address. I exchanged a number of letters with the City and met with the team putting together their submission to help identify and address these issues. Unfortunately, the City was not the successful municipality in its category.

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.



FPT Information and Privacy Commissioner Conference  
Regina, Saskatchewan - September 12-13, 2018





## ***Health Information Act***

We continued to receive a large number of requests under the *Health Information Act* this year, with a total of 29 files opened. Of these files

- eighteen were breach notifications received from the Department of Health and Social Services, the Hay River Health and Social Services Authority and the Northwest Territories Health and Social Services Authority pursuant to section 87 of the Act;
- three were breach of privacy complaints received from the public;
- two were requests to review a refusal to make corrections to information in a patient's chart;
- three were for the review of Privacy Impact Assessments submitted pursuant to section 89 of the Act;
- one was in relation to a request for access to a patient's own personal health information;
- one was a request for comment received from a health information custodian;
- one was an administrative file.

Most of the breach notification files were what would be considered minor breaches, most notably misdirected faxes and emails and the mishandling of communications with clients, usually involving only one person's personal health information. Others involved more serious breaches, including the theft of a laptop containing personal health information about almost every resident of the Northwest Territories and the report of the discovery of what appeared to be counselling and other personal health information in the Fort Simpson dump.

Breach notifications from health information custodians have also revealed a rather alarming number of prescription errors in which a prescription is issued in the wrong name. There was also one complaint from an individual who alleged that the health information custodian failed to comply with a directive provided to the custodian restricting access to the individual's health records.

The continued use of fax technology to communicate and to transfer health records continues to be worrisome. While human error will always be a factor which contributes to privacy breaches, the use of secure digital communication technology can significantly reduce the possibility of a breach as a result of such errors. Electronic transfers, of course,



can also be misdirected, but if the personal health information is transferred using secure digital technology the chances of a breach are greatly reduced. I continue to encourage health information custodians in the Northwest Territories to prohibit the use of fax machines when dealing with documents containing personal health information, except where absolutely necessary. There seems, however, to be a reluctance within the sector to make the change to more secure methods of communication.

---

*Data breaches and compromises are expensive, result in an enormous amount of collateral everyday life damage and are more common than inter-relationship bickering. .... [T]here is always room for improvement. While it is folly to believe that any company can be made 100% hack or leak proof, they can become harder-to-hit targets. Security can be baked into all processes--from onboarding to new product launches to the storing of key data. They are more avoidable than one might be led to believe, but it requires a sea change in attitude and more importantly a complete change in the way everything digital is done with security always foremost in any given process.*

*If You Have to Ask How Much a Data Breach Costs, You Can't Afford One, Adam Levin, Inc., August 19, 2019*

---



## REVIEW REPORTS

### *Access to Information and Protection of Privacy Act*

Eighteen Review Reports were issued under the *Access to Information and Protection of Privacy Act* in 2018/2019.

#### Review Report 18-178

<b>Category of Review:</b>	Privacy Complaint
<b>Public Body Involved:</b>	Department of Municipal and Community Affairs
<b>Sections of the Act Applied:</b>	Section 1, Section 40, Section 42, Section 43, Section 48
<b>Outcome:</b>	<ul style="list-style-type: none"> <li>- Recommendation to ensure that information gathered for the purpose of “duty to accommodate” are used solely for that purpose rejected.</li> <li>- Recommendation to ensure “duty to accommodate” and “disciplinary” issues are dealt with as separate processes rejected.</li> <li>- Other recommendations accepted or accepted in principle</li> </ul>

The Complainant was an employee of the public body who had some health issues. The public body requested and received a medical prognosis from the Complainant’s physician for the purpose of their duty to accommodate so that they could assess what, if any, accommodations were appropriate to assist the Complainant. The prognosis provided contained overly detailed information about the Complainant’s health history, treatment, and medication, among other things. The Complainant continued to have difficulties at work and was eventually required to attend a meeting to “discuss the medical prognosis received”. The discussion at the meeting, however, was disciplinary in nature and not related to the duty to accommodate process. A second meeting some months later in which information in the prognosis report was again used in a disciplinary proceeding. Discipline was imposed on the Complainant as a result, in part, of information contained in the prognosis.

The Information and Privacy Commissioner (IPC) found that the information gathered to address the public body’s duty to accommodate was improperly used in the discipline proceedings. Personal information collected by public bodies can only use personal



information for the purpose it was collected (or a consistent purpose) unless the individual consents to another use. The IPC found that the use of the information in the discipline process was not a consistent purpose. She further found that it was inappropriate for the public body to include information from the prognosis form in the letter of discipline given to the Complainant and shared with a number of officials. The public body had already conceded this point and had issued a new letter and asked everyone who had received the original letter to destroy it.

The IPC recommended that:

- a) records collected for the purpose of the GNWT's duty to accommodate are maintained separately from other personnel records and are sealed unless required to assess accommodations needed or the employee consents to the records being opened;
- b) access to such records be strictly limited to Duty to Accommodate Officers and the employee's immediate supervisor and that appropriate security measures are in place to ensure no unauthorized access;
- c) policies and procedures be amended as necessary to ensure that it is clear that records, and in particular medical records, collected for the purpose of evaluating a public body's duty to accommodate are to be used solely for that purpose;
- d) policies and procedures be amended as necessary to ensure that duty to accommodate issues and disciplinary issues are dealt with as separate processes
- e) steps be taken to ensure that the physicians are clear that a prognosis provided for the purpose of the GNWT's duty to accommodate should include only the information strictly necessary to allow the public body to assess any accommodations required for the employee.

## Review Report 18-179

<b>Category of Review:</b>	Access to Information
<b>Public Body Involved:</b>	Department of Health and Social Services
<b>Sections of the Act Applied:</b>	Section 1, Section 14(1)(a), Section 18(b), Section 23(1), Section 24 and Section 33
<b>Outcome:</b>	Recommendations accepted

The Applicant sought records relating to annual audits of regional authorities within the Child and Family Services division over a four-year period. There were significant delays in the provision of the response, and when it was provided, it was heavily redacted. The



Information and Privacy Commissioner assessed each item redacted and the exemption provision applied. She found:

- a) that the public body properly redacted personal information, the disclosure of which would have amounted to an unreasonable invasion of privacy;
- b) that the public body had not established that most of the information redacted pursuant to section 14(1)(a) (advice or recommendations to public bodies) met the criteria for such an exemption. She further found that the public body's exercise of discretion for those items that did meet the criteria did not include all of the relevant considerations. She recommended that most of the information redacted pursuant to this subsection be disclosed;
- c) that the public body did not establish that any of the redacted material, if disclosed could be reasonably expected to prejudice the use or results of a future audit. She recommended that most of the information redacted pursuant to section 18(b) be disclosed.

### Review Report 18-180

<b>Category of Review:</b>	Access to Information – Deemed Refusal
<b>Public Body Involved:</b>	Department of Justice
<b>Sections of the Act Applied:</b>	Section 6, Section 7, Section 8, Section 11, Section 26, Section 27
<b>Outcome:</b>	Recommendation accepted

The Applicant requested copies of records in relation to a dispute between himself and a third-party contractor also engaged by the Department. There were many delays in responding, largely because of errors by the Department when responding to the request. The records were eventually provided and no review of the actual response was, therefore, necessary. The IPC did, however, comment on the process and the errors made by the Department which contributed to the delayed response and recommended that the Department take steps to ensure that they adhere to the time frames set out in the Act.

### Review Report 18-181

<b>Category of Review:</b>	Correction to Personal Information
<b>Public Body Involved:</b>	Aurora College
<b>Sections of the Act Applied:</b>	Section 45(1), Section 45(2)
<b>Outcome:</b>	No Recommendations Made

The Applicant objected to comments made in a disciplinary letter put on his file which made reference to a specific medical condition and made statements about his willingness to co-



operate that were, in his opinion, not true. He was concerned that this “false information” then became a part of his personnel records and could be seen by any number of people in Human Resources and other departments. Also, in order to make a claim for Employment Insurance benefits, he was required to provide a copy of the letter to federal officials and he was concerned about how the information in the letter would affect his qualification for benefits and about the further disclosure of his personal information, true or not. The Applicant sought a correction to the personal information contained in the letter but the public body refused to make the corrections.

During the course of the review, the IPC suggested that the public body issue a second letter to the Applicant removing any reference to his personal health information and the public body agreed to do so. The Applicant accepted that letter as a partial solution, but maintained his request that a permanent correction be made on his personnel file.

The IPC found that while Section 45 of the Act gives an individual the right to request a correction to his or her personal information but public bodies have the discretion to refuse to make such corrections and are justified in refusing to make such corrections when:

- a) there is a dispute about whether there is an error or omission of fact concerning an applicant’s personal information;
- b) there is a third party’s recorded statement of fact regarding the applicant’s personal information, even if the recorded information is wrong;
- c) there is a third party’s opinion about the applicant.

The IPC found that the information that the Applicant sought to have corrected was an opinion about the Applicant and the public body was therefore justified in refusing to make the requested correction.

## Review Report 18-182

<b>Category of Review:</b>	Access to Information
<b>Public Body Involved:</b>	Department of Infrastructure
<b>Sections of the Act Applied:</b>	Section 22, Section 23(1), Section 23(2)(d), Section 23(2)(h)(I), Section 23(2)(i), and Section 24(1)(c)(ii)
<b>Outcome:</b>	Recommendations largely accepted with the exception of the recommendation to disclose a third party’s NWT Certificate of Registration number.

The Applicant sought information in relation to permits issued to a particular contractor for work done on properties owned by the Applicant over a particular period of time. He



received 9 pages of redacted records. The IPC reviewed each of the items redacted and found:

- a) that Section 22 (evaluative or opinion material about the Applicant collected to determine the Applicant's suitability or eligibility for employment) did not apply and recommended that information redacted pursuant to this section be disclosed;
- b) that some of the information withheld pursuant to section 23 (unreasonable invasion of privacy), was properly withheld, not all of it met the criteria for the redaction. She recommended the disclosure of some of this information;
- c) that the public body did not provide appropriate evidence to establish that information withheld pursuant to section 24 (financial or commercial information that would prejudice the competitive position of a third party) would cause harm to a third-party business. She recommended the disclosure of this information.

### Review Report 18-183

**Category of Review:** Access to Information  
**Public Body Involved:** Department of Infrastructure  
**Sections of the Act Applied:** Section 23(2)(d), Section 23(2)(h)(i), and Section 24(1)(b)(i)  
**Outcome:** Recommendations accepted

The Applicant requested copies of complaints filed against him by certain companies or individuals over a stated period of time. The public body identified eight (8) pages of responsive records which were provided to the Applicant, though with some redactions. The department relied on section 23 (disclosure would amount to an unreasonable invasion of a third party's privacy) for most of the material that was redacted. There was also some information redacted pursuant to section 24 (disclosure would harm a third party's business interests). The IPC found that the Department appropriately redacted most of the information withheld but recommended the disclosure of some additional information.

### Review Report 18-184

**Category of Review:** Privacy Complaint  
**Public Body Involved:** Department of Justice  
**Sections of the Act Applied:** Section 42, Section 47.1, Section 43, Section 48  
**Outcome:** Recommendations accepted

The Department of Justice failed to decommission the Complainant's government email address or to remove or adjust his permissions to access the PeopleSoft system at the end of his employment. As a result, the Complainant continued to have unauthorized access to personal information about his former staff through PeopleSoft long after his employment



responsibilities ended. The Complainant was further concerned that his government email address remained active and monitored by another employee for at least six months after his departure, resulting in a breach of his privacy.

The IPC found that the failure to properly decommission the Complainant's government email address amounted to a potential breach of the privacy of third parties sending email to the address, as well as of the Complainant's privacy. She further found that the Complainant's continuing access to the personal information of other employees in the PeopleSoft system constituted a clear breach of their privacy.

The IPC recommended a thorough review of policies and procedures around the management of email accounts. She further recommended that a technical solution be found which allows a former employee to continue to have access to his/her PeopleSoft account while preventing access to anyone else's information.

### Review Report 18-185

**Category of Review:** Access to Information  
**Public Body Involved:** Department of Education, Culture and Employment  
**Sections of the Act Applied:** Section 23(1)  
**Outcome:** Recommendations accepted

The Applicant requested a copy of a report prepared under the Harassment Free and Respectful Workplace Policy as a result of a complaint he had made. He was provided with partial access to the report, with identifying information of most third parties redacted on the basis that disclosure would constitute an unreasonable invasion of the privacy of those third parties. The IPC reviewed each item redacted from the report and made recommendations that some additional information be disclosed but agreed, for the most part, with the public body's decision to withhold other identifying information.

### Review Report 18-186

**Category of Review:** Access to Information  
**Public Body Involved:** Department of Municipal and Community Affairs  
**Sections of the Act Applied:** Section 1, Section 14(1)(a), Section 23, Section 24  
**Outcome:** Recommendations accepted in part and rejected in part

The Applicant made a request for "the whole of the 2017 Town of Norman Wells Municipal Report...and all notes and findings". The public body provided the Applicant with a number of records but many were partially redacted pursuant to section 14(1)(a), Section 23 and Section 24.





Most of the information withheld in this case was withheld pursuant to section 14(1)(a) which allows public bodies to withhold information where the disclosure could reasonably be expected to reveal advice, recommendations, analyses or policy options developed for a public body. The IPC held that findings of fact contained in an investigation report do not constitute “advice, recommendations or analyses” which would give rise to an exemption under section 14(1)(a). She recommended the disclosure of additional parts of the report.

### Review Report 18-187

**Category of Review:** Breach of Privacy  
**Public Body Involved:** Northwest Territories Housing Corporation  
**Sections of the Act Applied:** Section 40, Section 41(d), Section 42, Section 43, Section 48  
**Outcome:** Recommendations accepted

The Complainant had received a housing subsidy under a public housing program because of financial need. When applying for the housing subsidy, he provided the name of his previous landlord for the purpose of allowing the public body to do a background check as to his reliability and suitability as a tenant. Eventually the Complainant was able to overcome his financial difficulties and moved out of public housing. At some point the public body received information which suggested that the Complainant may have misrepresented his financial circumstances when he originally applied for the housing benefit and, months after the Complainant was no longer a tenant, sought to collect the full subsidy that the Complainant had received while a tenant. The Complainant discovered that after he had moved out of the unit, the public body had contacted his former landlord and, posing as a would-be new landlord, asked for and received information about the Complainant’s financial circumstances. The Complainant considered this to be an inappropriate collection of his personal information and filed a complaint with the OIPC.

The public body argued that they were required, under the *Financial Management Act* to investigate possible fraud stemming from the receipt of a public, needs-assessed financial benefit. While it was admitted that the public body had collected information from the former landlord, they denied that they held themselves out as doing a background check on a potential tenant. They also relied on the application form signed by the Complainant at the time of his application for the subsidy which included a consent to “conduct credit inquiries, income verifications, medical or family confirmations and reference checks”. The consent form did not include consent for the collection of information to investigate allegations of program fraud.

The IPC found that the consent to collection of personal information signed at the time application for public housing was, on its face, limited to “information required for the purpose of determining and verifying eligibility for social housing programs” and the



circumstances suggested that the consent was limited to the application process. She found that the consent to collect personal information of the tenant ended, at the latest, when the tenancy ended and there was no longer a valid contractual relationship between the public body and the tenant. The consent, therefore, did not authorize the collection of personal information after the end of the tenancy.

The IPC, however, also found that section 40( c) of the Act allows public bodies to collect information where the information relates directly to and is necessary for an existing program of the public body and that it was an important part of any subsidy program that there be a way to prevent abuse of the program. She found that the collection of information from the former landlord was authorized by this section. She further found that the use/disclosure of that information was authorized pursuant to section 48(d) of the Act which allows a public body to use or disclose personal information for the purpose of collecting a debt owed by an individual to the GNWT or one of its agents.

The IPC recommended that:

- a) the public body clearly set out the criteria for public housing in the application form;
- b) the public body amend the consent in the application form to make it clear that if the applicant is accepted as a tenant, the consent for the collection of personal information survives the application process so long as the applicant is a tenant of the organization;
- c) include in the consent a statement that one of the purposes for the collection of personal information is to allow the public body to ensure the integrity of the subsidy program
- d) ensure that in policy and practice, the collection of personal information is always done in good faith.

## Review Report 18-188

**Category of Review:** Request for Correction to Personal Information

**Public Body Involved:** Department of Education, Culture and Employment

**Sections of the Act Applied:** Section 44, Section 45(1), Section 45(2)

**Outcome:** No Recommendations Made

The Applicant made two requests to the Department of Education, Culture and Employment to correct information in relation to his applications for Student Financial Assistance (SFA). The Applicant had made several applications for SFA within one month. One of those applications was lost or misplaced by the Department. When the Applicant asked the department to make a note of this on his file, it agreed to put a note on his file to indicate



that he had requested this issue to be addressed. The Applicant sought to have the notation changed to indicate explicitly that the department had “lost” his application.

The second request for correction was in relation to the amalgamation of the Applicant’s several applications into one form. The Applicant argued that this was an improper alteration which affected his eligibility for funding. A note was made to the Applicant’s file acknowledging the concerns raised but this did not satisfy the Applicant who wanted the correction to reflect malfeasance on the part of the Department in attempting to “pass off” his three applications for funding as one.

The IPC found that the corrections requested by the Applicant were not corrections to his personal information. They were, instead, requests to correct the classification of an administrative error or action of the public body, which is not covered in the ATIPP Act. No recommendations were made.

### Review Report 18-189

<b>Category of Review:</b>	Privacy Complaint
<b>Public Body Involved:</b>	Department of Education, Culture and Employment
<b>Sections of the Act Applied:</b>	Section 42, Section 44
<b>Outcome:</b>	Recommendations accepted

The Department of Education, Culture and Employment mishandled several applications for funding submitted by the Complainant. The Complainant alleged that, as a result, his privacy was breached. The Department admitted error in handling the records. Two of the applications had improperly been treated as “transitory records” and not correctly saved to the Applicant’s file. After prompting from the Applicant, they recovered the emails in which these applications had been received and placed them on the Applicant’s file. A third application had been submitted on paper, however, could not be located. The staff noted that it had been received because it was reflected in the electronic notes for the client in its electronic system. The department concluded that the paper application had been incorrectly but securely destroyed as a “transitory” record.

The IPC found that the fact that the department could not account for the third application, which contained enough personal information to allow for identity theft if it landed in the wrong hands, amounted to a breach of privacy and recommended that the public body offer to pay for credit monitoring services for the Applicant for two years. She further found that there had been no breach in the mishandling of the other records. She did, however, recommend that the Department review and amend their policies and procedures with



respect to their information management practices and, in particular, to the classification of records as “transitory”.

### Review Report 18-190

<b>Category of Review:</b>	Access to Information
<b>Public Body Involved:</b>	Department of Justice
<b>Sections of the Act Applied:</b>	Section 23, Section 24
<b>Outcome:</b>	Recommendations largely accepted

The Applicant sought copies of correspondence and notes of two Department employees in which the Applicant was mentioned or discussed. He was not satisfied that the response received was complete and felt that some of the records had been doctored. He also questioned the application of sections 23 (unreasonable invasion of privacy) and 24 (harm to business interests).

The IPC held that there was no evidence to suggest that the response was either incomplete or doctored. She reviewed each of the redacted items and recommended the disclosure of additional information, particularly information withheld pursuant to section 23 where the information was more in the nature of business communications between the public body and a third party contractor, noting that there are many circumstances in which the disclosure of personal information will not amount to an unreasonable invasion of privacy.

### Review Report 18-191

<b>Category of Review:</b>	Access to Information - Extension of Time
<b>Public Body Involved:</b>	Northwest Territories Health and Social Services Authority
<b>Sections of the Act Applied:</b>	Section 7, Section 11
<b>Outcome:</b>	Recommendations accepted

The Applicant requested general information about the awarding of a tender for certain services in a community. The request was made on May 24, 2018. On May 28th, the Northwest Territories Health and Social Services Authority acknowledged the request and advised that because the request “may” result in a high volume of documents, it was extending the date for responding to the request pursuant to section 11 of the Act, and that the response would be provided no later than August 22nd. The Applicant objected to the extension of time and asked the IPC to review it.

The public body explained that the person in the organization who would normally have handled the documents in questions was away on leave which meant that access to the records was made far more difficult and would take much more time. While the IPC acknowledged that the absence of a key employee would clearly add to the time needed to



gather and review the responsive records, she was not satisfied that the public body had met the requirement of establishing that meeting the 30-day time limit for a response would “unreasonably interfere with the operations of the public body”. She made recommendations that the public body review and amend policies so as to address the issues raised in this review.

## Review Report 18-192

<b>Category of Review:</b>	Privacy Complaint
<b>Public Body Involved:</b>	Workers’ Safety and Compensation Commission
<b>Sections of the Act Applied:</b>	Section 40, Section 43, Section 48
<b>Outcome:</b>	Recommendations accepted with significant reservations

The Complainant was involved in a workplace incident that resulted in his injury and made a claim for compensation. Before the WSCC would accept his claim, they required him to undergo an independent evaluation by a specialist. To accommodate this evaluation, the WSCC obtained the Complainant's consent for the collection of 5 years of medical records but in fact collected more than 10 years of such records.

The WSCC argued that the consent that the Complainant signed at the time of his initial claim was sufficient consent for the collection of as much information as the WSCC felt was required to assess the claim and they were not bound by the time frame in the second, more specific consent.

The IPC found that there is a very high onus on the WSCC to fully and completely explain what information they will collect, how it will be used and to whom it will be disclosed, particularly because the WCA requires employees to report employment related injuries or diseases to the WSCC (Section 17). To make a report, the worker must complete and sign the Workers' Report of Injury which further requires the employee to sign a very general "consent" to the collection, use and disclosure of personal information. Further, by virtue of section 19 of the WCA, anyone who files a report of injury is deemed to have made a claim for compensation, whether or not that was the wish or intention of the worker. The IPC found that, in these circumstances, the consent included in the Report of Injury can never be relied on as true, knowledgeable consent because it is a requirement, not a choice. Consent requires choice and understanding to be valid. Consents have real legal consequences and should, therefore, be treated with the attention to detail and formality that such a waiver of personal rights deserves.

The IPC held that obtaining consent in the claim process must be far more transparent and claimants must be given the tools to understand how much of their right to control the



collection, use and disclosure of their personal information is being forfeited when making a claim for compensation. She made a number of recommendations to achieve this goal.

### Review Report 18-193

<b>Category of Review:</b>	Fees
<b>Public Body Involved:</b>	Department of Finance
<b>Sections of the Act Applied:</b>	None Referred To
<b>Outcome:</b>	No Recommendations Made

The Applicant sought a review of the fees assessed with respect to an Access to Information Request he had made for “all discipline records” held with respect to his employment with the GNWT. After collecting the responsive records, the Department assessed a fee of \$216.25 for 865 pages at \$0.25 per page. The Applicant objected to the fee on the basis that, to his knowledge, he had never been disciplined and that the Human Resources Manual requires that an employee be made aware of any disciplinary documents placed on his/her file. Finally, he pointed to the same manual which states that an employee is entitled to access to their own personnel records at no cost.

The department explained that most of the records identified as being responsive consisted primarily of emails between Department of Finance staff about how to respond to a disciplinary action involving the Applicant. While all formal documents relating to employee discipline are placed on the employee’s personnel file, copies of working documents, emails soliciting advice or discussing a situation are not.

The IPC was satisfied that the public body's interpretation of the request was a fair one and that the number of records was appropriately estimated and the fee assessed, therefore, appropriate as well. She suggested that if the Applicant wished to revise or clarify the request so as to focus only on formal disciplinary records in his personnel file, he should advise the public body so that they could adjust its fee estimate.

### Review Report 18-194

<b>Category of Review:</b>	Fees
<b>Public Body Involved:</b>	Department of Finance
<b>Sections of the Act Applied:</b>	Section 50, Regulation 12, Regulation 13
<b>Outcome:</b>	Recommendations accepted

The Applicant made a request for all information in relation to the employer’s “duty to accommodate” in connection with his return to work. The Department identified 212 pages



of responsive records and assessed a fee of \$53.00 (\$.25 per page). The Applicant objected to the fee assessed, based on two factors. The first is that he had been advised the previous year in relation to another ATIPP request that there were only 69 pages of “duty to accommodate” records. Secondly, he argued that there should be no fee because duty to accommodate records are required to be maintained on an employee’s personnel file and policy allows employees access to their personnel file without a fee.

The public body indicated that while a previous ATIPP request had identified approximately 69 pages of records with respect to the duty to accommodate the Applicant, the department continued to receive a high volume of emails from the Applicant with a variety of questions and concerns and the number of responsive records had therefore increased. They noted as well that while all formal documents relating to an employee’s “duty to accommodate” needs are placed on the employee’s personnel file, working documents and emails soliciting advice or discussing a situation are not included and that “most” of the responsive records fell in this category.

The IPC found that the number of responsive records was properly assessed by the Department. She recommended, however, that the fee be reduced by \$.25 for each of the responsive pages that originated from the Applicant’s personnel file.

### Review Report 19-195

<b>Category of Review:</b>	Privacy Complaint
<b>Public Body Involved:</b>	Northwest Territories Health and Social Services Authority
<b>Sections of the Act Applied:</b>	Section 40, Section 43, Section 48
<b>Outcome:</b>	Recommendations accepted

The Complainant was an employee of the Northwest Territories Health and Social Services Authority. He was required to take time off work to deal with some health issues. During his absence, his employer made several requests for medical prognoses in order to meet their duty to accommodate. In at least one instance, the request included statements about events in the workplace and some that had been observed outside of work. The Complainant felt that the information collected outside the workplace was improperly collected and certainly improperly disclosed. Not only was this information disclosed to his physician but because it was included in the request for prognoses, it was also seen by a number of his co-workers who had access to his personnel records.

The Health Authority argued that it had a “duty to inquire” to determine if the Complainant required any accommodation and that this justified the request for the prognoses. The IPC





recognized the “duty to inquire” but indicated that the collection of information about the employee outside of the workplace was inappropriate. She pointed out that it is a slippery slope when gossip and innuendo can be “collected” and then used by a public body to make decisions that will affect an individual in his employment setting.

To the extent that the Complainant’s information was properly collected, the IPC found that it was improperly disclosed in the request for prognosis. She recommended that the public body review its policies and processes around its “duty to inquire” and its “duty to accommodate” so as to limit the amount of information collected and used for these purposes and that information from third party sources be collected/used/disclosed only where absolutely necessary.



## ***Health Information Act***

The Office of the Information and Privacy Commissioner issued seven Review Reports under the *Health Information Act*.

### **Review Report 18-HIA04**

<b>Category of Review:</b>	Breach Notification
<b>Custodian Involved:</b>	Northwest Territories Health and Social Services Authority
<b>Sections of the Act Applied:</b>	Section 87
<b>Outcome:</b>	No Recommendations Made

The Northwest Territories Health and Social Services Authority (NTHSSA) notified the OIPC that an employee of the Yellowknife Region had improperly disclosed the personal health information of a client when assisting the client to make arrangements for a specialist’s appointment in southern Canada. The employee understood the client to be a GNWT employee or dependent and sent the client’s name, the date, and the place and time of the appointment to the GNWT Human Resources Benefit Officer to request authorization for the travel through the GNWT’s third party employee insurance plan. The client, however, was not a GNWT employee and the disclosure, therefore, resulted in a breach of the client’s





privacy. By the time that the Review Report was issued, NTHSSA had made changes to procedures to avoid a similar breach in the future. During the course of the review, other vulnerabilities were discovered and changes made to prevent the possibility of future breaches. No recommendations were made.

### Review Report 18-HIA05

<b>Category of Review:</b>	Privacy Complaint
<b>Custodian Involved:</b>	Northwest Territories Health and Social Services Authority
<b>Sections of the Act Applied:</b>	Section 8, Section 10, Section 11, Section 14, Section 87, Section 88
<b>Outcome:</b>	Recommendations accepted

The Complainant had, at one point, seen Dr. “A”, a family physician at one of Yellowknife’s primary care clinics. He was not happy with the service provided by this physician and began seeing Dr. “B”, also a family physician at the same clinic. Dr. “B” referred the Complainant to Dr. “C”, a specialist at the Stanton Territorial Health Medical Clinic. Thirteen months later, Dr “C” examined the Complainant and wrote a consultation report and sent it to Dr. A rather than to the referring physician, Dr. B. The Complainant was extremely upset that the information had been sent to the wrong doctor.

In addressing the complaint, NTHSSA advised that when a specialist completes an examination, standard practice is to return the specialist report to the patient's family doctor, as recorded in MediPatient, NTHSSA's electronic health record system. This practice allows specialist reports to be returned to the patient's assigned family doctor if a locum physician or a physician who is no longer at the clinic requests the report, ensuring the report is reviewed in a timely manner. In this case, Dr. “A” was listed as the Complainant’s family physician, notwithstanding that the Complainant had made a considered and intentional decision to see another physician and hadn’t seen Dr. “A” for almost two years. It was the Custodian’s position that there had been no error or breach of privacy.

NTHSSA referred the IPC to a number of informational brochures but could not provide any confirmation that the Complainant had been provided with copies of these brochures or that anyone had explained the “team based” approach used by the clinics. It is clear that no-one had advised him that Dr. “A” had been assigned to be his family physician. The IPC made three recommendations with respect to changes required to ensure that clients understand how their information will be used and disclosed within the authority. She further recommended that NTHSSA implement a practice of having front end staff confirm the identity of the patient’s primary care physician each time a patient makes and appointment.



## Review Report 18-HIA06

<b>Category of Review:</b>	Request for Correction
<b>Custodian Involved:</b>	Hay River Health and Social Services Authority
<b>Sections of the Act Applied:</b>	Section 119, Section 120(1), Section 125, Section 126, Section 127
<b>Outcome:</b>	Recommendation rejected

The Applicant sought a correction to personal health information in his chart with the HRHSSA. He suffers from chronic pain but felt that his doctors were not listening to him when he told them of his pain. He therefore asked for a copy of his records and discovered that he had been labelled as a "drug seeker" and "known narcotic abuser", labels which he strongly disagreed with. He asked HRHSSA to correct the information on his file by removing certain information, including several references to medical information about his partner, references to other family members, references to his alleged "drug seeking" and "doctor shopping" and a physical description of him that he considered unprofessional. While adjustments were made to the records to remove references to third parties, HRHSSA refused to make most of the requested corrections.

The public body explained that the term used to describe the Complainant's physical attributes was a medical classification based on a number of measurable factors and that it was not a comment on the Complainant's appearance. During the course of the review process, however, they agreed to remove the reference to this term and instead substituted other medical terminology.

With respect to the references to the Complainant's alleged drug seeking behaviour, the IPC reviewed the sections of the HIA which allow individuals to ask for a correction to their medical records. She pointed out that a Custodian is entitled to refuse to make the correction where the individual seeking it has not demonstrated that the record contains an error, if there is a dispute of fact between the individual and the Custodian, or if the information is a medical opinion, reasonably held by the Custodian or its agents. The IPC found that the refusal to make the corrections was an appropriate response under the Act. As a result, no recommendations were made about these requested corrections.

The IPC did comment, however, on the inclusion of information on the Complainant's file which appears to have been received from a third party. This entry was different than other references in the Applicant's records in that it came from a third party who was neither an employee or agent of the custodian. It was, therefore, not a "professional opinion or opinion that a custodian has made in good faith". The IPC felt that it was more akin to



gossip than medical opinion and recommended that this reference be removed from the Complainant's record.

### Review Report 19-HIA07

**Category of Review:** Privacy Complaint  
**Custodian Involved:** Hay River Health and Social Services Authority  
**Sections of the Act Applied:** Section 38, Section 28(2)  
**Outcome:** "HRHSSA is committed to accepting your recommendations"

This complaint arose when the Hay River Health and Social Services Authority (HRHSSA) disclosed 10 years' of the Complainant's health information records to the Workers' Safety and Compensation Commission (WSCC) when he had signed a consent for only 5 years' of records. When HRHSSA eventually responded to the inquiries of the IPC to obtain an explanation, they conceded that the additional records had been sent out in error. No additional explanation and no indication of any steps taken to prevent a similar error in the future were provided.

The IPC found that the disclosure of the extra five years' of medical information was in breach of sections 38 of the Act (disclosure without required explicit consent), 28(2) (prohibiting the disclosure of more personal health information than reasonably necessary to meet the purpose of the disclosure). She also found that the Custodian's "Release of Patient Information Policy" was badly outdated (it had not been revised since the coming into force of the Health Information Act). Furthermore, they had not followed that policy because they had not documented the disclosure as required.

The IPC recommended that HRHSSA take immediate steps to establish policies to implement the requirements of the HIA with regard to disclosure of personal health information, as well as other policies as required to comply with the HIA. She recommended that at the same time the HRHSSA review and update all relevant forms to ensure consistency of naming and correct cross-referencing in policies.

Any kind of consent, including implied consent, must be knowledgeable.

REVIEW REPORT 18-HIA05



## Review Report 19-HIA08

<b>Category of Review:</b>	Privacy Complaint
<b>Custodian Involved:</b>	Northwest Territories Health and Social Services Authority
<b>Sections of the Act Applied:</b>	Section 20(1), Section 38,
<b>Outcome:</b>	Agreement only to “engage with the appropriate departments across the GNWT to obtain necessary advice, collaboration and advance this important work”

The Complainant, an employee of the GNWT, experienced a psychotic break and ended up being admitted to the hospital. In the process of attempting to return to work, his employer requested several medical prognoses over a period of several months. Two of the prognoses provided by NTHSSA contained detailed and specific information about diagnosis, medications, suggested medical follow-up and community supports being provided to the Complainant. While the Complainant had consented to the disclosure of his information for the purposes of the employer’s duty to accommodate, he did not intend that the Custodian would disclose his specific diagnosis or details with respect to his medication or any other specific medical information. He asked the OIPC to review whether or not too much information was provided to the employer by the physicians who completed the prognoses forms.

The IPC examined the requirements for a valid consent to the use or disclosure of personal information as contained in section 20 of the Health Information Act and found that, although the consent provided by the Complainant covered some of the required elements, it did not include all of the elements needed for a valid consent. There was nothing in the consent form itself in which the “purposes” of the disclosure were made clear or that indicated that the Complainant understood the purposes, and there was no statement contained in the consent that the Complainant could withhold or withdraw consent, all of which is required for a valid consent pursuant to section 20. All of the information disclosed, therefore, was improperly disclosed.

Even if the consent had been valid, the IPC found that too much information was disclosed - information which was not required by the Complainant’s employer to assess accommodations required to assist him to return to work. The complaint, therefore, was well founded.



She recommended that:

- a) NTHSSA establish formal policies and guidelines with respect to the kind of information that should and should not be included in a prognosis requested by an employer in relation to a return to work or accommodation process
- b) NTHSSA work with the appropriate authorities in the GNWT to amend the consent in the Request for Medical Prognosis form to ensure that it meets the requirements of section 20(3) of the Act or, in the alternative, that NTHSSA create its own form of consent for this purpose and require clients to sign that consent before completing requests from employers for prognoses;
- c) all medical personnel who might be required to complete medical prognosis forms, including nursing staff, physicians and specialists, be provided with specific training in relation to the proper way to respond to such requests.

### Review Report 19-HIA09

<b>Category of Review:</b>	Commissioner Initiated Review
<b>Custodian Involved:</b>	Hay River Health and Social Services Authority
<b>Sections of the Act Applied:</b>	Section 8, Section 10, Section 11, Section 85, Section 137(1), Section 154
<b>Outcome:</b>	“HRHSSA agrees with all of your recommendations but unfortunately cannot commit to full implementation”

The HRHSSA contacted the OIPC by phone on October 26th to advise that there had been an improper disclosure of the personal health information of several clients and that an investigation was being conducted and a full report would be provided when the investigation was complete. Unreasonable delays by the Authority in providing additional information, coupled with the need to confirm the nature of the breach and determine level of compliance under the Health Information Act, led the OIPC to initiate a formal review pursuant to section 137(2) of the Act.

The privacy breach was originally discovered by HRHSSA as part of a performance review that also identified gaps in procedure. To clearly identify suspected breach occurrences, the HRHSSA undertook an audit of related business activities dating back approximately six months, specifically to April 1, 2017. The audit revealed that the privacy of eight (8) clients was breached between October 10 and October 30, 2017.

The IPC found that the combination of the lack of clear and prescribed process, the deviation from expected process, errors in directing files to the wrong specialists, the over-sharing of information, the lack of oversight by management, and the redundant manual



processing of PHI resulted in inappropriate use and/or disclosure of the personal health information of eight clients with associated risks to privacy and security of the information.

The IPC recommended that:

- a) current policies and procedures for processing of personal health information be reviewed to ensure they are documented as formal, prescribed processes, and are made easily available to staff for reference and clearly reflect the expected information and handling requirements;
- b) operational oversight be instituted to ensure privacy principles are adhered to when handling PHI, and that discrepancies are addressed in a timely manner;
- c) the Authority conduct a general privacy audit of its operations, to identify incidents of non-compliance with legislation, to determine risks to PHI, identify solutions and implement plans to eliminate, mitigate or actively manage known privacy and security issues;
- d) all new and existing staff receive annual privacy training as is required by Ministerial policy directive.

### Review Report 19-HIA10

<b>Category of Review:</b>	Access to Information
<b>Custodian Involved:</b>	Northwest Territories Health and Social Services Authority
<b>Sections of the Act Applied:</b>	Section 6(2), Section 94, Section 97, Section 99, Section 100,
<b>Outcome:</b>	Recommendations accepted

The Applicant made a request to the Northwest Territories Health and Social Services Authority for access to a copy of an “encounter record” on the WOLF EMR. The Custodian provided the Applicant with a 42-page print-out. The Applicant, however, who was familiar with the EMR system, was not satisfied with the response provided and gave detailed instructions to NTHSSA on how to access the screen that was of interest to him. The HIA refused to provide a screen shot of the requested page. They argued that sections 99 and 100 protected the “technical configuration and data architecture” of the information systems. They argued that the care provider’s “work desk” is an internal view of business information, including limited personal health information, and as such is a proprietary view intended for use by authorized health care providers in managing their individual practices. Furthermore, they noted that screen shots are not an approved means of disclosing personal health information from the EMR or any electronic health information system.

NTHSSA argued that the specific screen shot requested by the Applicant was not a “record” as defined in the Act but that it was, rather a “computer program, an electronic health information system or another mechanism that creates a record”. They asserted, as well, that the Records Coordinator who routinely prepares responses to requests for access to



personal health information does not have the privileges within the EMR necessary to access the screen of interest to the Applicant.

The IPC found that the information displayed by the EMR on the computer screen is not the computer program itself or another mechanism that creates a record, but the output of an executed computer program. Furthermore, she found that the requested screen shot could reasonably be reproduced by NTHSS using its normal equipment and expertise and that creating a copy of the screen shot would not unreasonably interfere with its operations.

She recommended that the custodian respond to the Applicant's access request under the HIA and/or ATIPP, as the case may be. She further recommended that NTHSS establish a process to forward non-standard access requests to its HIA/ATIPP Coordinator for due consideration.







## TRENDS AND ISSUES MOVING FORWARD

These are exciting times for the Office of the Information and Privacy Commissioner. The amendments to the *Access to Information and Protection of Privacy Act* will create one of the most progressive pieces of access and privacy legislation in Canada and our office is excited for the new provisions to come into effect. We are already in the process of adjusting our procedures to meet the new requirements and will undoubtedly have to continue to make adjustments once the provisions come into effect and we learn more about how they will affect us. The amendments do, however, change the access and privacy landscape dramatically. Not only our office, but all public bodies as well, will need to make significant changes in their approach to the legislation. There will need to be a concerted and focussed effort to give municipalities the resources, knowledge and tools they need to comply with the legislation once they are added to the list of public bodies subject to the Act. Public bodies will need to be more aware of and attuned to access and privacy issues.

### Municipalities

Among the most significant of the amendments to the Act are those provisions which set the groundwork for municipalities to be included as public bodies under the Act. I am well aware that our local governments are concerned about the affect this will have on them, both financially and operationally. I certainly understand their concerns. That said, the Northwest Territories is one of the last jurisdictions in Canada to address the need for access and privacy legislation at the local government level. Municipalities large and small throughout the country have long been required to comply with such legislation and transparency and protection of personal privacy at the local level is as important as it is at the Territorial level.

Bringing municipalities under the Act will require careful planning, a reasonable implementation period, appropriate training and, above all, adequate resources to ensure that municipalities will be in a position to effectively meet their obligations under the Act. If not already done, I would strongly suggest that an implementation plan be put into place and that there be a significant investment made, not only in training but also in ensuring that local governments have the information management tools they need to adequately comply with the law.







## Public Bodies

Another significant change contained in the amendments to the *Access to Information and Protection of Privacy Act* is the power given to the Information and Privacy Commissioner to make orders. No longer will the IPC only make recommendations which are easily ignored by public bodies. The new provisions give the Information and Privacy Commissioner the power to make binding orders on public bodies which can be filed in the Supreme Court of the Northwest Territories and enforced the same way as any Court Order. The consequences, therefore, of not providing clear, detailed and complete submissions to the OIPC during the review process may well result a binding order based on inadequate information. While public bodies have been getting away with providing only cursory submissions when the IPC could only make recommendations, this will simply not be enough when the IPC is making binding orders. Public bodies will, therefore, need to step up when making submissions to the IPC during the review process, including providing legal argument to justify their position, and outlining all of the considerations which go into the exercise of discretion where applicable. Failure to do so will have significant implications.

I therefore recommend that steps be taken ahead of implementation to ensure that senior staff and ATIPP Co-ordinators in every public body are provided with training in relation to how to make submissions to the OIPC. There will undoubtedly be a learning curve for everyone involved, including the OIPC, but much can be done to make the transition as smooth as possible.

## The Office of the Information and Privacy Commissioner

The new provisions in the *Access to Information and Protection of Privacy Act* will also have a significant impact on the work of our office. As noted in the Commissioner's Message, the amendments will create considerable additional work and put additional pressure on the office to ensure that all deadlines are met. One of the implications of giving the Information and Privacy Commissioner the power to make orders is that the validity of those orders can be questioned if the orders are not made within the time frames provided for in the legislation. The office currently has a backlog of almost a full year. We are working as hard as we can right now to clear that backlog so that we can start under the new provisions with a clean slate.

The amendments also add new responsibilities for the Information and Privacy Commissioner, including



- reviewing and commenting on notices under section 5.1 when public bodies are proactively required to give the public notice of significant harm to the environment or to the health or safety of the public;
- reviewing and commenting on mandatory breach notifications from public bodies;
- reviewing and commenting on Privacy Impact Assessments completed by public bodies with respect to proposed enactments, systems, projects, programs or services involving the collection, use or disclosure of personal information;
- approving extensions of time for public bodies to respond to a Request for Information of more than 20 business days;
- a mandate to provide public education about access and privacy matters.

In order to ensure that this expanded mandate can be met, I have requested an additional four staff, including a Case Review Officer, two Investigators and a Communications Specialist. This staff will ensure that the added responsibilities, combined with the shortened time frames will not derail the purposes and intent of the new provisions or of the legislation as a whole.

## Review of Policies

With the coming into force of the new provisions to the ATIPP Act, is an opportune time for a comprehensive review of GNWT policies and procedures with respect to digital records. As was demonstrated by the case of the stolen laptop, there are many policies that are simply missing or are not being followed when it comes to electronic files. In that case, the very act of downloading huge datasets containing personal information and personal health information of thousands of residents onto a portable device, whether or not it was encrypted or password protected, should have been flagged as a serious departure from existing policy/procedure requiring extra security measures. It was not so flagged because the existing policies are unclear and not well enforced. This is not just a Department of Health and Social Services issue. This is a government wide issue.

As noted in my Annual Report last year, there still does not appear to be any GNWT policy that addresses employee use of personal devices, or the use of personal (and potentially insecure) email accounts, or the use of text messaging for conducting GNWT business. These are issues that are coming up time and again in my reviews, particularly as they relate to



privacy issues. They are, however, also extremely critical issues in terms of the need to document and preserve government records. I strongly recommend that this review take place as soon as possible.

### The Continued Use of Fax Technology in the Health Sector

Another issue that continues to repeat, particularly in connection with mandatory breach notifications under the *Health Information Act*, is the use of fax technology to transfer records containing personal information and personal health information of clients and patients. While the number of breach incidents as a result of misdirected faxes is down somewhat, this type of breach continues to occur with disturbing regularity. Personal health information is some of the most sensitive of personal information and it should be handled accordingly. Communication by means of encrypted email or other secure electronic transfer systems should be the default for all employees in the health sector. There is simply no excuse for the continuing breaches caused by fax transmissions being sent to the wrong place. Health care professionals need to do a better job to protect the personal health information of their patients.



**Commissaire à l'information et à  
la protection de la vie privée des  
Territoires du Nord-Ouest**

**RAPPORT ANNUEL  
2018/2019  
Résumé**





# Table des matières

<b>MESSAGE DE LA COMMISSAIRE .....</b>	<b>5</b>
<b>RAPPORT FINANCIER .....</b>	<b>11</b>
<b>BILAN DE L'ANNÉE .....</b>	<b>12</b>
<b>TENDANCES ET ENJEUX – POUR ALLER DE L'AVANT .....</b>	<b>16</b>





## MESSAGE DE LA COMMISSAIRE



Au début de l'exercice financier, mon bureau anticipait une année bien remplie, et notre anticipation s'est avérée. Parallèlement à nos travaux de résolution des plaintes au sujet de la protection de la vie privée et d'examen des questions d'accès à l'information, nous avons formulé des conseils à l'Assemblée législative et aux ministères sur les politiques et les questions de conformité, les lois, les modifications législatives et les nouveaux programmes.

Chaque année, les questions d'accès à l'information et de protection de la vie privée sont toujours plus complexes et difficiles, et les organismes publics doivent composer avec un nombre toujours croissant de demandes d'accès à l'information. La transition vers les dossiers numériques est en cours dans la plupart des secteurs du gouvernement, et je constate un intérêt croissant du public à l'égard des activités gouvernementales, comme en témoigne l'augmentation constante du nombre de demandes de renseignements adressées à mon bureau. Les membres du public sont beaucoup plus exigeants aujourd'hui qu'ils ne l'étaient il y a quelques années seulement en ce qui a trait au type d'information qu'ils s'attendent à recevoir au sujet du gouvernement et de ses activités. Les institutions démocratiques du monde entier se doivent maintenant d'être transparentes : la confiance du public dans le gouvernement est étroitement liée à la capacité des élus d'être transparents. Les Téoïis ne font pas exception, et démontrent un intérêt croissant à l'égard de leur gouvernement et des efforts qu'il déploie pour remplir ses divers mandats.





Au cours des deux dernières années, le dossier de la vie privée a pris un tournant que Michael McEvoy, commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, a qualifié de « bouleversement radical », suivant les révélations sensationnelles sur Facebook et Cambridge Analytica, et la façon dont ces deux entités ont recueilli et utilisé des données personnelles pour influencer diverses campagnes électorales. Ces révélations, en plus des centaines d'atteintes à la vie privée très médiatisées qui ont eu des conséquences sur des millions d'individus, en plus de milliers d'autres atteintes à la vie privée moins publicisées qui se produisent presque quotidiennement, ont permis de conscientiser le public aux questions relatives à la protection de la vie privée. Les sondages montrent que les Canadiens sont plus conscients des problèmes de confidentialité que jamais, et qu'ils sont plus attentifs à leur propre vie privée.

Dans la plupart des cas, la transmission d'informations personnelles aux organismes gouvernementaux n'est pas facultative. Si nous voulons accéder à des soins de santé ou à des services éducatifs, ou si nous souhaitons obtenir un permis de conduire ou du soutien social, nous n'avons d'autre choix que de divulguer des renseignements personnels à ces organismes publics. Si le gouvernement manque à son obligation de protéger ces informations, il en découlera inévitablement une perte de confiance du public. En matière de protection de la vie privée, les gouvernements ne peuvent plus s'en tenir à des vœux pieux : les organismes publics doivent mettre la protection de la vie privée à l'avant-plan dans toutes les sphères de leur fonctionnement.

Les feux seront bientôt braqués sur ces obligations avec l'entrée en vigueur du projet de loi 29, Loi modifiant la *Loi sur l'accès à l'information et la protection de la vie privée*, qui a été approuvé en première et en deuxième lecture en 2018. Ce



projet de loi représente l'aboutissement du travail entamé en 2012 et constitue le premier examen complet de la Loi depuis son entrée en vigueur le 31 décembre 1996. Il contient de nombreuses nouvelles initiatives intéressantes, notamment les dispositions nécessaires pour faire en sorte que la Loi s'applique aux administrations municipales des Territoires du Nord-Ouest. Au moment d'écrire ces lignes, le projet de loi avait été adopté en troisième lecture et avait reçu la sanction royale. Les modifications adoptées devraient entrer en vigueur, souhaitons-le, au cours des prochains mois. À l'étape de l'étude en comité, le projet de loi a été largement révisé; les amendements moderniseront considérablement le fonctionnement de notre commissariat ainsi que la façon de gérer les questions relatives à l'accès aux renseignements et à la protection de la vie privée aux Territoires du Nord-Ouest. Ces changements comprennent notamment :

- a) Le passage d'un « pouvoir de recommandation seulement » du commissaire à l'information et à la protection de la vie privée à la capacité d'émettre des ordonnances contraignantes qui ont force exécutoire;
- b) Les bases nécessaires pour étendre la Loi aux municipalités;
- c) D'obliger les organismes publics à divulguer sans délai tout risque de préjudice grave pour l'environnement ou pour la santé ou la sécurité du public lorsque cette divulgation est nettement dans l'intérêt public;
- d) L'exigence que les organismes publics divulguent à la commissaire les atteintes importantes à la vie privée qui concernent une ou plusieurs personnes, et de les aviser en cas de risque réel de préjudice grave à leur endroit;



- e) L'exigence que tous les organismes publics préparent une évaluation des facteurs relatifs à la vie privée lors de la promulgation ou de la rédaction d'un texte, d'un projet, d'un programme, ou de l'élaboration d'un système ou d'un service proposés qui comprendrait la collecte, l'usage ou la divulgation de renseignements personnels, et la présente à la commissaire à l'information et à la protection de la vie privée pour examen et commentaire;
- f) Le passage du délai accordé à la commissaire à l'information et à la protection de la vie privée pour terminer un examen de 180 jours civils à 90 jours ouvrables (environ quatre mois et demi);
- g) L'exigence que les organismes publics demandent à la commissaire à l'information et à la protection de la vie privée une prolongation des délais s'ils ont besoin de plus de 20 jours pour répondre à une demande de renseignements selon les délais impartis;
- h) L'ajout, au mandat de la commissaire à l'information et à la protection de la vie privée, de la tâche de sensibiliser le public aux questions d'accès à l'information et de protection de la vie privée.

Il s'agit de modifications d'importance qui changeront radicalement la donne, et mon bureau attend avec impatience l'entrée en vigueur de la nouvelle Loi. Le passage des « recommandations » aux « ordonnances » est particulièrement important et exigera des organismes publics qu'ils apportent un soin considérable à leurs soumissions au commissariat lors des processus d'examen, et qu'ils accomplissent un bien meilleur travail pour expliquer les raisons qui sous-tendent leur pouvoir discrétionnaire lorsqu'ils refusent l'accès à l'information. Le pouvoir d'émettre des ordonnances obligera mon bureau à être clair, concis, et précis lorsqu'il émet une ordonnance; quant à lui, le processus d'examen devra devenir



plus formel, et les soumissions devront être présentées suivant un calendrier strict.

Les Territoires du Nord-Ouest seront la cinquième compétence canadienne où le commissaire à l'information et à la protection de la vie privée pourra rendre des ordonnances exécutoires, après la Colombie-Britannique, l'Alberta, l'Ontario et l'Île-du-Prince-Édouard. Le commissaire à l'information et à la protection de la vie privée du gouvernement fédéral est également en train d'obtenir un tel pouvoir'. Il s'agit d'un changement positif qui, à mon avis, est des plus sensés dans le monde numérique actuel.

L'année 2018-2019, étant donné les atteintes à la vie privée — y compris deux particulièrement médiatisées dans le domaine de la santé, en a été une particulièrement occupée pour le commissariat. La première concernait un ordinateur portatif volé contenant des renseignements médicaux personnels sur presque tous les résidents des TNO. La seconde était la découverte d'anciens dossiers contenant des informations personnelles de nature délicate et, dans certains cas, des renseignements personnels sur la santé, prétendument retrouvée au dépotoir de Fort Simpson. Outre ces deux infractions fortement publicisées, le nombre de plaintes suivant une infraction et les notifications d'infraction obligatoires en vertu de la *Loi sur les renseignements sur la santé* ont continué d'augmenter, comme en témoigne le nombre de rapports d'examen publiés en vertu de la Loi.

Je suis très heureuse d'avoir accueilli Dylan Gray, qui s'est joint au commissariat à titre de commissaire adjoint et d'enquêteur le 1<sup>er</sup> mars de cette année. Comme



M. Gray occupait auparavant un poste de spécialiste principal de la protection des renseignements personnels au ministère de la Santé et des Services sociaux, ses connaissances du domaine de la santé nous seront des plus utiles. Son embauche signifie que nous avons maintenant deux enquêteurs au sein de notre équipe, et nous ne ménagesons aucun effort pour rattraper le retard que nous continuons d'accumuler.

Je me dois également de souligner le travail crucial qu'effectue notre gestionnaire de bureau, Lee Phypers, toujours organisée et positive. Son dévouement et sa connaissance de notre travail sont essentiels au bon fonctionnement du commissariat.



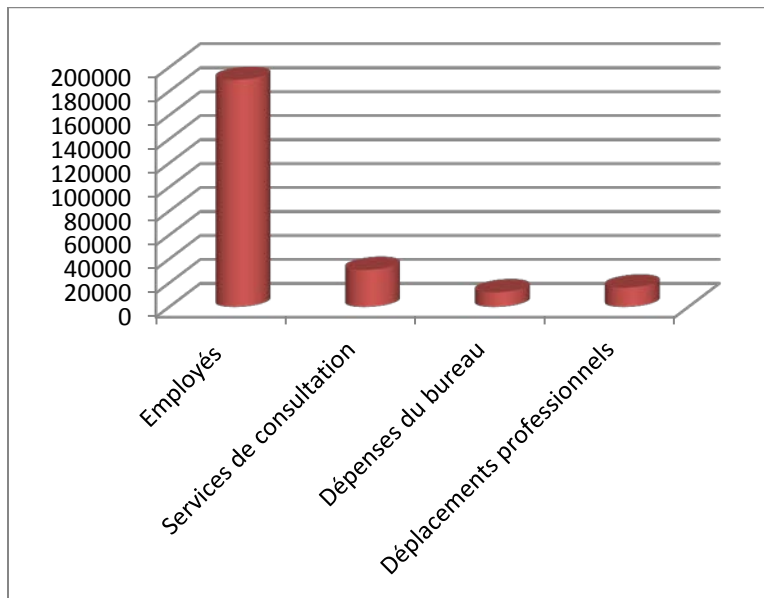
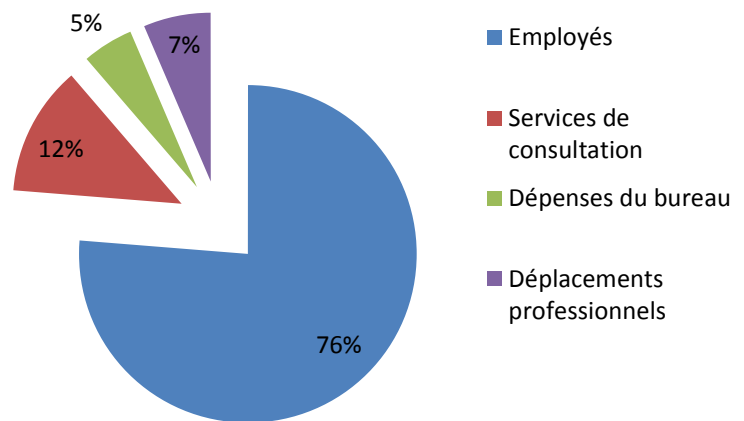
Participation au groupe de commissaires à la conférence sur l'accès et la vie privée de l'Université d'Alberta 2019



## RAPPORT FINANCIER

Pour l'exercice 2018-2019, le total des fonds (fonds cumulés) dépensés pour le fonctionnement du commissariat à l'information et à la protection de la vie privée des Territoires du Nord-Ouest et du Nunavut s'élevait à 248 442,20 \$. La ventilation détaillée de ces coûts est présentée dans les tableaux ci-dessous

### Commissariat à l'information et à la protection de la vie privée Dépenses 2018 / 2019





## BILAN DE L'ANNÉE

Au cours de l'exercice 2018-2019, le Commissariat à l'information et à la protection de la vie privée a ouvert un total de 84 dossiers.

### Loi sur l'accès à l'information et la protection de la vie privée

Du 1<sup>er</sup> avril 2018 au 31 mars 2019, 55 dossiers ont été ouverts en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*. Les dossiers ouverts se répartissent dans les catégories suivantes :

Demandes d'examen — Accès à l'information	19
Demandes d'examen – Refus présumés	8
Notification d'atteinte à la protection des données provenant d'un organisme public	7
Demandes d'examen – Atteinte à la vie privée	6
Consultations — Demandes de commentaires	5
Affaires diverses	3
Demandes d'examen — Évaluation des droits	2
Affaires administratives	2
Notification d'atteinte à la protection des données provenant d'un tiers	1
Demandes d'examen — Prorogation de délai	1
Demandes d'examen — Consultation d'une tierce partie	1

Encore une fois, ces données indiquent que la majorité des dossiers qui ont été ouverts sont des demandes d'examen des réponses obtenues suivant des demandes d'accès à l'information. Il y a eu une augmentation significative du nombre de demandes d'examens concernant l'incapacité des organismes publics à répondre à une demande de renseignements dans les 30 jours, comme l'exige la Loi (refus présumé). La plupart de ces problèmes ont été résolus sans qu'un examen officiel soit nécessaire. Cette situation indique cependant que des organismes publics commencent à avoir de la difficulté à répondre à leurs obligations.



Cette année, j'ai été heureuse de pouvoir travailler avec la Ville de Yellowknife à l'évaluation des incidences sur la vie privée de la participation au Défi des villes intelligentes d'Infrastructure Canada. La capitale téninoise était finaliste pour le prix d'au plus 5 millions de dollars et, dans sa proposition définitive, devait évaluer toute incidence sur la vie privée que son projet pourrait soulever. La Ville et moi avons d'abord entretenu une correspondance avant que je ne rencontre les membres de l'équipe chargée de la proposition pour les aider à s'occuper des questions relatives à la vie privée. Yellowknife n'a malheureusement pas récolté les honneurs dans sa catégorie.

En plus des questions qui ont donné lieu à l'ouverture de dossiers, nous avons naturellement traité, sur une base quotidienne, nombre d'appels de personnes qui souhaitent obtenir des renseignements de base au sujet de la Loi; nous avons répondu à leurs demandes immédiatement, sans ouvrir de dossier.



Conférence du commissaire FPT à l'information et à la protection de la vie privée.  
Regina, Saskatchewan - 12-13 septembre 2018





## ***Loi sur les renseignements sur la santé***

Cette année encore, la *Loi sur les renseignements sur la santé* nous a tenus occupés : 29 dossiers ont été ouverts en vertu de cette Loi. Parmi ces dossiers, mentionnons :

- Dix-huit notifications d'atteinte à la protection des données reçues du ministère de la Santé et des Services sociaux et de l'Administration des services de santé et des services sociaux des Territoires du Nord-Ouest en vertu de l'article 87 de la Loi;
- Trois plaintes pour atteinte à la vie privée ont été reçues du public;
- Deux demandes d'examen suivant un refus d'apporter des correctifs au dossier médical d'un patient;
- Trois évaluations des répercussions sur la vie privée en vertu de l'article 89 de la Loi;
- Une demande d'accès d'un patient qui souhaitait consulter son propre dossier médical;
- Une demande de commentaire reçu d'un dépositaire des renseignements médicaux;
- Un dossier administratif.

La plupart des dossiers de notification d'atteintes à la vie privée pourraient être qualifiés de violations mineures, comme des télécopies et des courriels mal adressés, ou une mauvaise gestion des communications avec les clients, impliquant généralement des renseignements médicaux personnels sur la santé d'une seule personne. D'autres portaient sur des infractions plus graves, notamment le vol d'un ordinateur portable contenant des renseignements médicaux personnels sur presque tous les habitants des TNO, sans oublier la découverte de ce qui semblait être des dossiers de counseling et d'autres renseignements médicaux personnels dans la décharge de Fort Simpson.

Des dossiers de notification d'atteintes à la vie privée commises par le dépositaire de renseignements sur la santé ont révélé un nombre préoccupant de cas où une ordonnance médicale est émise pour le mauvais patient. Un autre dossier a été ouvert par un résident qui accusait le dépositaire de renseignements sur la santé de ne pas s'être conformé à une directive limitant l'accès à son dossier médical.

L'utilisation continue du télécopieur pour la communication et le transfert de dossiers médicaux reste problématique. Bien que l'erreur humaine puisse entraîner des violations de la



vie privée, l'utilisation d'une technologie numérique sûre réduit grandement les risques. Bien sûr, les transferts électroniques peuvent également être mal dirigés, mais les risques d'infraction sont considérablement réduits si on favorise une technologie numérique sécurisée. Je continue à encourager les dépositaires des renseignements sur la santé à interdire l'utilisation du télécopieur pour traiter des informations personnelles, sauf en cas d'absolue nécessité. Il semble toutefois que le secteur soit réticent à faire la transition vers des méthodes de communication plus sûres.





## TENDANCES ET ENJEUX – POUR ALLER DE L’AVANT

Le Commissariat à l’information et à la protection de la vie privée traverse une période particulièrement stimulante. Les modifications apportées à la *Loi sur l’accès à l’information et la protection des renseignements personnels* feront de notre loi l’une des plus progressistes en la matière au pays, et notre bureau est impatient de voir les nouvelles dispositions entrer en vigueur. Nous sommes déjà en train de rajuster nos procédures pour répondre aux nouvelles exigences et nous continuerons sans aucun doute à faire des rajustements lorsque les nouvelles dispositions seront en vigueur et que nous saurons plus précisément comment elles nous affectent. Notons cependant que ces amendements modifieront radicalement les enjeux de l’accès aux renseignements et de la protection de la vie privée. Non seulement notre bureau devra-t-il adopter une nouvelle approche à l’égard de cette loi, mais tous les organismes publics devront en faire autant. Un effort concerté sera nécessaire pour doter les municipalités des ressources, connaissances et outils nécessaires afin qu’elles se conforment à la loi lorsqu’elles y seront assujetties. Les organismes publics devront être mieux renseignés et plus sensibles aux questions d’accès à l’information et de protection de la vie privée.

### Les administrations municipales

Parmi les modifications les plus importantes qui ont été apportées à la Loi, mentionnons les dispositions qui prévoient l’intégration des municipalités à la catégorie des organismes publics assujettis à la Loi. Je suis bien consciente que nos administrations locales s’inquiètent des répercussions que les modifications auront sur elles, tant sur le plan financier que sur le plan opérationnel, et je comprends leurs préoccupations. Cela étant, les Territoires du Nord-Ouest sont l’une des dernières sphères de compétence au Canada à étendre sa *Loi sur l’accès à l’information et la protection de la vie privée* aux administrations municipales. D’un océan à l’autre, les municipalités, grandes et petites, sont tenues depuis longtemps de se conformer à de telles lois. La transparence et la protection des renseignements personnels compte autant à l’échelle locale que territoriale.



Étendre l'application de la Loi aux municipalités exigera une planification minutieuse, une période de mise en œuvre raisonnable, une formation appropriée et, surtout, des ressources suffisantes pour que les municipalités soient en mesure de s'acquitter efficacement de leurs obligations en vertu de la loi. Si ce n'est déjà fait, je suggérerais fortement qu'un plan de mise en œuvre soit rédigé et que des investissements conséquents soient réalisés, non seulement pour la formation, mais également pour garantir que les organismes concernés disposent des outils de gestion de l'information nécessaire pour se conformer à la loi.

### Organismes publics

Le pouvoir de rendre des ordonnances conféré à la commissaire à l'information et à la protection de la vie privée est un autre changement important apporté à la Loi. Le commissariat ne fera plus que formuler des recommandations que les organismes publics peuvent facilement ignorer. Les nouvelles dispositions lui donnent le pouvoir de rendre des ordonnances exécutoires à l'encontre d'organes publics qui peuvent être déposées devant la Cour suprême des Territoires du Nord-Ouest et exécutées de la même manière que toute ordonnance judiciaire. Par conséquent, le fait de ne pas fournir de réponses claires, détaillées et complètes au commissariat pendant le processus d'examen pourrait bien donner lieu à une ordonnance exécutoire fondée sur des informations insuffisantes. Auparavant, les organismes publics qui ne fournissaient que des réponses partielles à la commission pouvaient se tirer d'affaire facilement, puisque le commissariat n'avait qu'un pouvoir de recommandation. Cette époque sera bientôt révolue. Les organismes publics devront maintenant faire preuve de sérieux lorsqu'ils présentent leurs observations au commissariat pendant le processus d'examen, notamment lorsqu'ils s'appuient sur un avis juridique pour justifier leur position et qu'ils soulignent toutes les considérations qui entrent dans l'exercice de leur pouvoir discrétionnaire, le cas échéant. Faute de quoi, les conséquences pourraient être graves.

Je recommande que les mesures nécessaires soient prises pour garantir que les cadres supérieurs et les coordonnateurs de l'accès à l'information et à la protection de la vie privée de tous les organismes publics reçoivent une formation sur la façon de présenter des observations au commissariat à l'information et à la protection de la vie privée. Tous les intervenants concernés devront sans aucun doute passer par une courbe d'apprentissage, y compris le



personnel du commissariat, mais nous pouvons faire en sorte que la transition se déroule sans heurt.

## Commissariat à l'information et à la protection de la vie privée

Les nouvelles dispositions de la *Loi sur l'accès à l'information et la protection de la vie privée* auront des répercussions importantes sur le travail de notre bureau. Comme indiqué dans le message de la commissaire, les modifications imposeront une charge de travail supplémentaire considérable et exerceront une pression accrue sur le bureau si l'on souhaite respecter tous les délais. En effet, l'une des conséquences du passage d'un pouvoir de recommandation seulement à un pouvoir d'émettre des ordonnances contraignantes, est que la validité d'une telle ordonnance peut être mise en doute si elle n'est pas rendue selon les délais fixés par la Loi. À l'heure actuelle, le retard qu'accuse le commissariat atteint presque une année complète. Nous travaillons d'arrache-pied pour venir à bout de ce retard afin que nous puissions nous conformer aux nouvelles dispositions dans les meilleures conditions possible.

Les modifications confèrent également de nouvelles responsabilités à la commissaire à l'information et à la protection de la vie privée, notamment :

- examiner et commenter les avis publiés en vertu du paragraphe 5.1 lorsque des organismes publics doivent divulguer au public le risque d'un préjudice grave pour l'environnement ou pour la santé ou la sécurité du public;
- examiner et commenter les avis de violations obligatoires provenant d'organismes publics;
- examiner et commenter les évaluations des facteurs relatifs à la vie privée effectuées par des organismes publics à propos des promulgations, textes, projets, programmes, systèmes ou services pour lesquels des renseignements personnels sont recueillis, utilisés, ou divulgués;
- approuver toute prolongation de plus de 20 jours ouvrables du temps accordé à un organisme public pour répondre à une demande de renseignements;
- le mandat de sensibiliser le public aux enjeux de l'accès à l'information et aux renseignements personnels.



Afin de pouvoir remplir ce mandat élargi, j'ai demandé l'embauche de quatre employés supplémentaires, notamment un agent d'examen des cas, deux enquêteurs et un spécialiste des communications. Ce personnel veillera à ce que les nouvelles responsabilités, combinées à des délais plus courts, ne nuisent pas à la lettre et à l'esprit des nouvelles dispositions de la Loi, ou de la Loi dans son ensemble.

### L'examen des politiques

Avec l'entrée en vigueur des nouvelles dispositions de la *Loi sur l'accès à l'information et la protection de la vie privée*, le moment est venu de procéder à un examen complet des politiques et procédures du GTNO en matière de documents numériques. Comme l'a démontré le cas de l'ordinateur portatif volé, en matière de dossiers électroniques, soit les politiques nécessaires sont inexistantes, soit elles ne sont pas suivies. Dans ce cas, le simple fait de télécharger d'énormes ensembles de données contenant des renseignements personnels et des renseignements personnels sur la santé de milliers de résidents sur un appareil portatif, peu importe qu'il soit crypté ou protégé par un mot de passe, aurait dû être signalé comme une grave dérogation à la politique et aux procédures existantes nécessitant des mesures de sécurité supplémentaires. L'incident n'a pas été signalé parce que les politiques existantes ne sont pas claires et ne sont pas correctement appliquées. Et il ne s'agit pas d'un problème propre au ministère de la Santé et des Services sociaux : c'est un problème à l'échelle du gouvernement.

Comme je l'ai indiqué dans mon rapport annuel de l'année dernière, il ne semble toujours pas exister de politique du GTNO concernant l'utilisation d'appareils personnels par les employés, de comptes de messagerie personnels (et potentiellement non sécurisés), ou l'utilisation de messagerie texte pour mener les activités ministérielles du GTNO. Ces questions reviennent sans cesse dans mes rapports, particulièrement en ce qui concerne les questions de protection de la vie privée. Ce problème soulève d'autres questions cruciales, notamment la nécessité de documenter et de préserver les archives du gouvernement. Je recommande fortement que cet examen ait lieu dès que possible.



## L'utilisation du télécopieur dans le secteur de la santé

L'utilisation du télécopieur pour transférer des dossiers contenant des informations personnelles et des renseignements sur la santé, surtout à la lumière des avis obligatoires d'atteinte à la vie privée en vertu de la *Loi sur les renseignements sur la santé*, continue de causer régulièrement problème. Bien que le nombre d'incidents résultant de télécopies mal envoyées ait légèrement diminué, ce type de violation continue de se produire avec une régularité inquiétante. Les renseignements médicaux personnels sont parmi les informations les plus confidentielles qui soient, et ils devraient être traités en conséquence. Par défaut, tous les employés du secteur de la santé devraient communiquer par courrier électronique crypté ou par tout autre système de transfert électronique sécurisé. Absolument rien ne peut excuser les violations continues causées par les télécopies envoyées au mauvais numéro. Les professionnels de la santé doivent faire un meilleur travail pour protéger les renseignements sur la santé de leurs patients.

