



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

2016-2017 annual report

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT
HEALTH INFORMATION ACT





OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
NORTHWEST TERRITORIES

P.O. Box 383
Yellowknife, NT
X1A 2N3

July 19, 2017

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, 2016 to March 31st, 2017.

Yours very truly

Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories

/kb

In Yellowknife: 867-669-2976 Toll Free: 888-521-7088 Fax: 867-920-2511 Email: admin@atipp-nt.ca



TABLE OF CONTENTS

COMMISSIONER'S MESSAGE	6
ACCESS TO INFORMATION AND PROTECTION OF PRIVACY – A BRIEF OVERVIEW	10
Access to Information and Protection of Privacy Act	10
Health Information Act	13
THE YEAR IN REVIEW	15
General	15
Access to Information and Protection of Privacy Act	15
Health Information Act	17
REVIEW RECOMMENDATION	19
Access to Information and Protection of Privacy Act	
Review Recommendation 16-144	19
Review Recommendation 16-145	19
Review Recommendation 16-146	20
Review Recommendation 16-147	21
Review Recommendation 16-148	22
Review Recommendation 16-149	23
Review Recommendation 16-150	25
Review Recommendation 16-151	25
Review Recommendation 16-152	26
Review Recommendation 16-153	27
Review Recommendation 16-154	28
Review Recommendation 16-155	29
Review Recommendation 17-156	29
Review Recommendation 17-157	30
Review Recommendation 17-158	31
Review Recommendation 17-159	34
Health Information Act	
Report 16-HIA01	35
Report 16-HIA02	38
Report 16-HIA03	40
EMERGING ISSUES	43







THE COMMISSIONER'S MESSAGE



2017 marks my 20th year as the Information and Privacy Commissioner of the Northwest Territories which also means that it is the 20th anniversary of the coming into effect of the Access to Information and Protection of Privacy Act. The job I took on in 1997 is very different than the job I do today. When I began, “Access to Information” was undeniably the focus of the job. Over the years, as the value of information increased and technology advanced, “Protection of Privacy” took a primary role. In recent years, however, “Access to Information” issues are again becoming prominent. This seems to be the general trend throughout the country. While the public continues to be very concerned about the

ability of governments to protect the personal information collected in the course of government business, changing political realities, the growing value of information as an asset and the growing demand of the general public that governments be transparent and accountable have all brought increasing focus back to the Access to Information side of the equation. As noted by the Nova Scotia Information and Privacy Commissioner in her 2016-2017 Annual Report:

Twenty-four years ago, the world was a different place. In 1993 there were only 130 websites. Today there are one billion. Google wasn't founded until 1998 and Facebook wasn't created until 2004. Big data was the realm of scientists and dreamers.

One thing is for certain. Strong access and privacy legislation is increasingly vital to the maintenance of our democratic ideals as the world changes in ways no one would have imagined in 1997.



I completed my first three reviews under the new *Health Information Act* during the year. Two of these arose out of privacy complaints and the third came to me as a result of a notification pursuant to section 87 of the Act. What became clear as a result of these reviews is that the legislation is dense, complicated and hard to interpret which means that the time and effort necessary to conduct a review is more significant than doing a similar review under the *Access to Information and Protection of Privacy Act*. It is to be hoped that as we all become more familiar with the Act and its interpretation, this time commitment will be reduced. Each of my reviews resulted in a conclusion that health information custodians in the public sector were far from compliant with the Act and that much work needed to be done. The amalgamation of six regional health authorities created some huge holes in the new Territorial Authority's ability to respond to Access to Information Requests under the *Access to Information and Protection of Privacy Act*. That said, I am beginning to see some progress on compliance with the *Health Information Act* and some move toward consistency throughout the system which can only be a good thing. There is, however, still much more to be done. In particular, it appears that the electronic systems being used by the Department of Health and the NT Health and Social Services Authority still do not have the functionality necessary to allow patients the right to control access to and use of their personal health information as mandated by the *Health Information Act*.

It was encouraging to see the first comprehensive review of the *Access to Information and Protection of Privacy Act* proceed this year and to participate in some in-depth consultations with the Department of Justice surrounding efforts to update and modernize the legislation to reflect modern day realities. The review was long overdue but I am very pleased to see the serious efforts being made to make the legislation more functional in today's world and encouraged to hear that consideration is being given to some very progressive and even innovative possibilities. I look forward to continuing my work with the Department as they move toward the tabling of new legislation in the coming months.

The rapidly increasing workload being addressed by my office underlines the need for a review, as well, of the resources dedicated to the office. 2016-2017 saw a 40% increase in the number of files opened by my office under the *Access to Information and*



Protection of Privacy Act. In fact, the overall case load of the office has increased 157% since 2013/14*. This trend is holding and even accelerating in the first quarter of 2017-2018. While I work diligently to stay on top of this rapidly increasing workload, it is a losing cause. As a result, I have been unable to complete reviews within the mandated 6 months and the backlog is increasing month by month. I renew my request for an increase in my budget sufficient to fund the addition of an Assistant Commissioner/ Investigator so that my office can continue to meet its legislated mandate.

I took advantage, this year, of the rare opportunity to attend an international conference entitled “Transparency for the 21st Century” hosted by the Information Commissioner of Canada in Ottawa in March. This conference covered topics such as International Perspectives on the Right to Know, the Role of the Fourth Estate and Transparency and Indigenous Rights. I also continued my participation in Canada Health Infoway’s Pan Canadian Forum which has been ongoing for a number of years and which focuses on privacy in the health sector. Finally, at the invitation of the Privacy Commissioner of Canada, I also participated in a meeting organized by his office to discuss the concept of “consent” and privacy in today’s connected world. All of these conferences and meetings were informative and interesting. The most important meeting of any year, for me, however, is the annual meeting of my federal, provincial and territorial counterparts which this year was held in Ontario. Our discussions ranged from a cross-country review of developments in access and privacy, discussions on the challenges raised by changes in government, public interest disclosures, open government and big data and surveillance.

I was also pleased this year to sign my name to a joint submission to the public consultation on the modernization of Canada’s national security framework. The preparation of this submission was spearheaded by the Office of the federal Privacy Commissioner and was signed by all of my provincial and territorial counterparts. The submission addressed a number of privacy issues, including domestic and international information sharing, the collection and retention of communications metadata,

* 30 files opened in 2013/14, 69 under ATIPP plus 8 HIA in 2016/17



proposals to make it easier for law enforcement to access customers' subscriber information and encrypted communications, and the need for greater transparency and oversight of agencies involved in national security.

In closing, I would like to acknowledge and thank my assistant, Lisa Phypers, for her continued support and assistance. Her dedication, hard work and cheery disposition make my job so much easier .





ACCESS TO INFORMATION AND PROTECTION OF PRIVACY – A BRIEF OVERVIEW

The Access to Information and Protection of Privacy Act

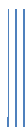
The *Access to Information and Protection of Privacy Act* enshrines two principles:

1. public records must be accessible to the public; and
2. personal information must be protected by public bodies.

It outlines the rules by which the public can obtain access to public records and establishes rules about the collection, use and disclosure of personal information collected and maintained by public bodies in the Northwest Territories. It applies to 41 departments, crown corporations, local housing organizations and other agencies in the NWT.

Access to Information

Part I of the legislation provides the public with a process to obtain access to most records in the possession or control of public bodies. This right of access is so important to the maintenance of open and accountable government that access to information laws have been deemed to be quasi-constitutional in nature. When the public can see how government is functioning and how they are doing their work, they are better able to participate in government and to hold government and governmental agencies to account. The right of access to government records is not, however, absolute. There must be some exceptions and these limited and specific exceptions are set out in the legislation. Most of the exceptions function to protect individual privacy rights and proprietary business information of the companies which do business with the Government of the Northwest Territories. The exceptions also function so as to allow Ministers and their staff to have free and open discussions as they develop policies and deal with issues.




Requests for Information must be in writing and delivered to the public body from whom the information is sought. When a Request for Information is received, the public body must first identify all of the records which respond to the request, then assess each record and determine what portion of that record should be disclosed and what might be subject to either a discretionary or a mandatory exception. This is a balancing act which is sometimes difficult to achieve. The response must be provided to the Applicant within 30 days.

When an Applicant is not satisfied with the response provided by the public body, he/she can apply to the Information and Privacy Commissioner (IPC) to review the response given. The full process is outlined in the chart that follows.

Protection of Privacy

Part II of the Act provides rules for when and how public bodies can collect personal information, what they can use such information for once it has been collected and in what circumstances that information can be disclosed to another public body or the general public. It requires that all government agencies maintain adequate security for the personal information it holds and that that personal information is only available to those who need it to do their jobs.

This part of the Act also gives individuals the right to ask for personal information held by a public body to be corrected.



PRIVACY IS NOT ABOUT WHETHER OR NOT YOU
HAVE SOMETHING TO HIDE. PRIVACY IS ABOUT
HAVING CONTROL OVER WHAT YOU WANT TO
SHARE AND WHAT YOU WANT TO KEEP TO
YOURSELF.

— [- Aral Balkan](#)



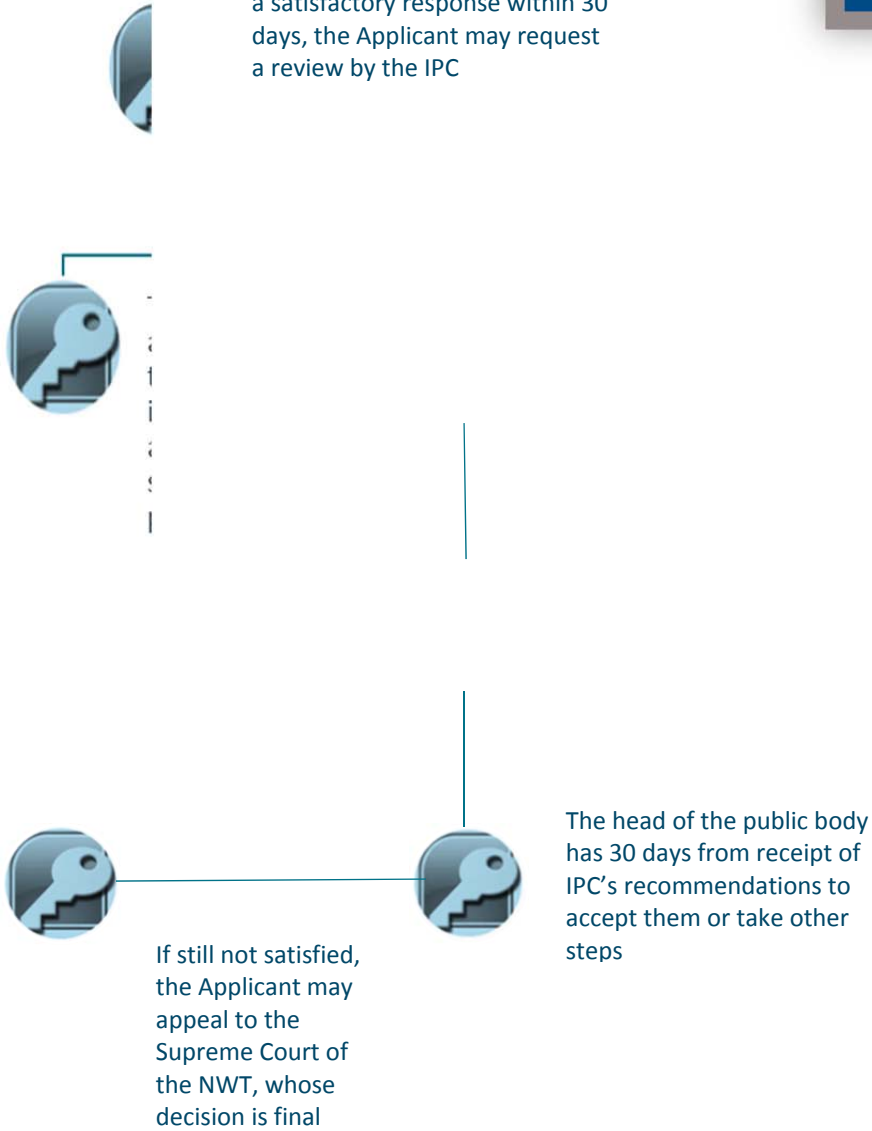
THE ACCESS TO INFORMATION PROCESS

Health Information Act



Protecting Your Privacy in the Health System

If the public body fails to provide a satisfactory response within 30 days, the Applicant may request a review by the IPC



The Health Information Act



The *Health Information Act* came into effect on October 1st, 2015. The purpose of this Act is to govern the collection, use and disclosure of personal health information and to provide for the protection of such information. It is intended to recognize both the right of the patient to access and control who else has access to their personal health information and the need of those providing health care to collect, use and disclose that information for the purpose of providing health care.

This legislation applies to all records containing the health information of an identifiable individual in the custody or under the control of a health information custodian, as defined in the Act, whether that custodian operates in the public sector or the private sector.

The Act allows medical practitioners to assume, in most situations, that an individual who seeks health care from them has provided implied consent to the collection, use or disclosure of personal health information for the purposes of providing health care to the patient. This is, however, contingent on the practitioner having satisfied himself or herself that the patient is knowledgeable about how this information is to be collected, used and disclosed. In any case in which the patient has expressly indicated that the practitioner is not to rely on implied consent, practitioner must obtain the patient's express consent to collect, use or disclose personal health information, except in very limited situations, such as emergency health care. The Act also gives the patient the right to put conditions on who has access to his or her personal health records and can direct, for example, that one or more practitioners, nurses, clerical staff or other employee in any particular office be prohibited from accessing that patient's file.

Overarching all of these provisions is the clear direction set out in the Act 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 *Health Information Act* also provides patients with the right to access any record containing his or her own personal health information which is in the care or custody of a health information custodian. A process for requests for information similar to that in the *Access to Information and Protection of Privacy Act* is included in the Act, though it is somewhat more complicated and the time lines for responding are potentially far longer than in the case of the ATIPP Act.

A request for personal health information is also subject to the payment of fees, which contrasts with a request for personal information under the *Access to Information and Protection of Privacy Act* which allows only for the recovery of photocopying costs in the case of a request for personal information.



If a patient believes that there is an error in his or her medical health records, a request can be made to have that information corrected.

Where a person believes that a health information custodian has improperly collected, used or disclosed his or her personal health information, if they are not satisfied with the response they receive to a request for access to their personal health information, or if there is a dispute about the correction of medical health records, the *Health Information Act* allows the individual the right to request the Information and Privacy Commissioner to review the matter. With only a few minor differences, the review process is the same as under the *Access to Information and Protection of Privacy Act*. Once the review is completed, the health information custodian must make a decision to accept the recommendations made or take other steps within 30 days. The rights of appeal under the *Health Information Act* are quite different than the rights of appeal under the *Access to Information and Protection of Privacy Act*. For one thing, the right of appeal applies to breach of privacy issues in addition to access to information matters, and correction of personal information disputes. Secondly, and perhaps more significantly, the Information and Privacy Commissioner has the right to launch an appeal of a decision of a health information custodian to the courts.

Also new with the *Health Information Act* there is a positive duty imposed on health information custodians to give notice to any individual whose personal health information has been used or disclosed contrary to the provisions of the Act, is lost or stolen or if it is altered, destroyed or otherwise disposed of without authorization. This notice must also be given to the Information and Privacy Commissioner, who may choose to investigate the breach.

WE BEGIN, THEN, WITH THE NEED TO BALANCE THE PATIENT'S RIGHT TO CONTROL WHO CAN USE AND DISCLOSE HIS/HER PERSONAL HEALTH INFORMATION WHILE STILL MEETING THE NEEDS OF THE HEALTH PROVIDER TO DELIVER HEALTH SERVICES. NEITHER OF THESE PURPOSES TRUMPS THE OTHER. THEY MUST BE BALANCED.

REPORT 16-HIA01



THE YEAR IN REVIEW

General

The Office of the Information and Privacy Commissioner opened a total of 69 files in 2016/2017, a 40% increase from 2015/2016. This is in addition to 42 new files in Nunavut, which represents a 25% increase in files for that jurisdiction as well. In the first month and a half of the 2017/2018 fiscal year, 24 new files have been opened in the Northwest Territories and 15 for Nunavut. Needless to say, the resources of this one-person office serving two jurisdictions are being stretched beyond capacity. As a result, applicants and complainants are being subjected to significant delays in dealing with their matters and it is often taking much longer than the 180 days provided for in section 31(3) for the Commissioner to complete a report and provide recommendations. This increase in numbers is not unexpected or unusual. The north is following the trend of all Canadian jurisdictions, as access and privacy issues become ever more important and populous participation in government expands.



Access to Information and Protection of Privacy Act

The OIPC opened 61 files under the *Access to Information and Protection of Privacy Act* during 2016/2017, compared to 43 in 2015/16. These files can be divided into a number of categories:

Access to Information Matters	
General Requests for Review	19
Deemed Refusal Complaints	7
Extension of Time Complaints	4
Fees	1
Third Party Objections	1
Breach of Privacy	
General Privacy Breach Complaints	11
Public Body Breach Notifications	1
Other Breach Notifications	2
Comments/Consultations	5
Miscellaneous inquiries/requests	7
Administrative	3



Some of the increase in numbers can be attributed to multiple requests being received from one source over short periods of time – sometimes all directed at one public body but often to multiple public bodies. This also accounts for a number of “deemed refusal” matters as public bodies which are not used to this kind of volume are simply not being able to keep up with demand. Several public bodies received multiple Requests for Information within a short time frame and were unable to respond within the requisite 30 days.

These numbers also suggest a bit of a shift from privacy complaints, back to access to information. This is also a trend throughout the country. Although the public is still very concerned about their privacy, there has been an increased focus on access to information issues in recent months.

The “Miscellaneous” files included speaking engagements, access requests that were not perfected or were outside the scope of the jurisdiction of the office and files that were resolved very quickly and without the need for a full review.

Fifteen Review Recommendations were issued.



Health Information Act

The *Health Information Act* came into force on October 1st, 2015. In fiscal 2016/2017 my office opened eight files under the *Health Information Act*. Of these:

- a) three were breach notifications received from various branches of the amalgamated Northwest Territories Health and Social Services Authority.
- b) two involved the submission of Privacy Impact Assessments as per section 89(2) of the Act;
- c) one was a comment to the Minister of Health on the department's Mental Health Care Action Plan;
- d) two were administrative files, including one representing an ongoing discussion between my office and the Northwest Territories Health and Social Services Authority on issues arising out of the Act and the Reports issued by my office during the year.

Three formal reports containing recommendations under the *Health Information Act* were issued in 2016/2017.

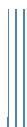
In my last Annual Report, I was quite critical of the failure of the Department of Health and its agencies to address the new requirements under the *Health Information Act* and of the lack of any significant effort to educate the public about their rights and responsibilities under the legislation. Things appear to be improving, though slowly. There has been some progress on the development of system-wide standards, policies and procedures as required by section 8 of the Act. I have also seen a significant upturn in the number of breach notifications being received which suggests there is more awareness about what constitutes a breach under the Act. Moreover, these breaches are being properly handled and steps are being taken to prevent re-occurrences. I have also observed, in the last few months that the clinics, in Yellowknife at least, have some posters on the wall informing patients about their basic rights under the Act.

There are, however, still some significant gaps that need to be addressed. The biggest one is that the systems utilized by the Northwest Territories Health and Social Services Authority does not have the functionality to ensure that the rights granted to individuals under the Act are capable of being met. Even though the Act clearly gives patients the right to limit access to their personal health information, it appears that none of the electronic medical record keeping systems in use in the Northwest Territories, at least at the government level, have the capacity



to mask either parts or the whole of an individual's record. Nor can the system be configured so that one or more medical care practitioners can be prevented from accessing or viewing a particular individual's medical records.

While there has been some improvement in the last year there is much more yet to be done. Undoubtedly, the learning curve is very steep and it will take us a while to get to basic compliance. All this is to say that it is fairly safe to predict that the *Health Information Act* is likely to generate a lot of work for the OIPC over the next few years.



REVIEW RECOMMENDATIONS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT

REVIEW RECOMMENDATION 16-144

Category of Review:	Privacy Complaint
Public Body Involved:	A Local Housing Organization (NWT Housing Corporation)
Sections of the Act Applied:	Section 43, Section 48
Outcome:	No Privacy Breach, No Recommendations Made

The Complainant complained that the Local Housing Organization was disclosing to his neighbors that he had been complaining to the landlord about other tenants and calling the police. The IPC found that the Landlord was required, by law, to inquire into complaints made by tenants and to take appropriate action. The Landlord in this case did conduct such investigations, but that there was nothing to suggest that the Landlord had identified the Complainant as the person who had made the complaint.

REVIEW RECOMMENDATION 16-145

Category of Review:	Privacy Complaint
Public Body Involved:	Department of Transportation
Sections of the Act Applied:	Section 40, Section 48
Outcome:	Recommendation to remove cameras not accepted Other recommendations accepted

A complaint was received about the use of video surveillance cameras in the Driver and Vehicle Licensing Office in Yellowknife. The Department claimed that the purpose of the cameras was the security and safety for employees, noting that members of the public sometimes behave badly and that employees are quite frequently subjected to verbal abuse and sometimes physically threatening behavior. They argued that the cameras allowed the Supervisor to monitor or detect potential situations involving violence, abuse and harassment and the images had the potential to assist in an investigation in the case of an incident. They pointed out, as well, that the design of the office was such that without cameras, employees were unable to see if there was anyone waiting in the waiting room or to identify anyone attempting to deliver something to them behind their secure door.



The cameras did not record, but were monitored in “real time”. It was possible to take and save a “screen shot” but this was a fairly complicated process that took 20 – 30 seconds to accomplish.

The Information and Privacy Commissioner found that the surveillance cameras, whether or not they actually recorded, were not “necessary” to provide protection to either the staff or the public and there was no evidence at all that they added to the safety of either the public or of employees. Furthermore, the cameras were being used to monitor and discipline staff and to spy on customers waiting in the waiting area. Even if the collection of personal information in the form of video images could be said to be “necessary” to the functions of the office, these secondary uses of the information were clearly contrary to the Act. The IPC made a number of recommendations including the removal of the cameras in favour of other, less privacy invasive options to address both safety concerns and the physical limitations of the space.

REVIEW RECOMMENDATION 16-146

Category of Review:	Access to Information
Public Body Involved:	Department of Human Resources
Sections of the Act Applied:	Section 23(2)(d)
Outcome:	Recommendations Accepted with exception of one

The Applicant sought access to information with respect to workplace complaints made against him. The Department of Human Resources provided a response, but some third party information had been redacted. The Applicant argued that the third party had given up his right to privacy by filing a harassment complaint against the Applicant, particularly in light of the fact that, in the Applicant's opinion, the third party had egregiously misrepresented the facts. The IPC agreed, for the most part, with the public body's attempt to protect the personal information of the third party, but recommended the disclosure of some additional information.



REVIEW RECOMMENDATION 16-147

Category of Review:	Access to Information
Public Body Involved:	Department of Justice
Sections of the Act Applied:	Section 23
Outcome:	Recommendations Accepted

An Applicant requested a copy of a video record of an incident in which his image had been captured on security footage in a government office. The Department decided that they were unable to provide the Applicant with a copy of the video in question because it included the images, and therefore the personal information, of third parties and the disclosure of the videos would amount to an unreasonable invasion of the privacy of those individuals. Apart from this, they did not have the technology or the expertise to edit the recording so as to blur or otherwise mask the faces of others who were captured in the video. They did, however, allow the Applicant and his lawyer to view the recording.

The Applicant sought a review of the decision not to provide him with a copy of the record. He argued that the incident occurred in a public space which everyone knew, or ought to have known, was under video surveillance and, as a result, there was no reasonable expectation of privacy. The Applicant, having been given the opportunity to view the record, also argued that one of the four camera angles showed only himself, the two court officers and an RCMP officer and no other members of the public. He argued that these individuals being employees of the GNWT or the Government of Canada should have no expectation of privacy in their workplace as law enforcement officers.

The IPC found that the public body took reasonable efforts to provide the Applicant with access to his own personal information while protecting the privacy of the many third parties also depicted in the video recordings and that it would have been an



unreasonable invasion of the privacy of the other third parties depicted to provide the Applicant with an unedited copy of the recording. She found, however, that if a public body conducts video surveillance, it must be done in such a way as to accommodate the right of the public to seek access to those videos. In other words, the technology employed should allow for editing of images so as to mask faces of third parties. She recommended that, in this case, the Department seek to have the video appropriately edited by an outside agency. She further recommended that the Department take steps to ensure that it has the necessary technological capacity to be able to provide an applicant with a copy of his or her personal information captured in video surveillance while protecting the privacy of others whose images are also captured.

REVIEW RECOMMENDATION 16-148

Category of Review:	Access to Information - Extension of Time
Public Body Involved:	Department of Human Resources
Sections of the Act Applied:	Section 8, Section 11, Section 23(1), Section 26(1)
Outcome:	No recommendations made

The Applicant sought copies of notes taken at a meeting held between certain individuals on a particular date. The public body indicated that they required additional time to consult with third parties pursuant to section 11 and extended the time to respond accordingly. The Applicant objected to the extension of time and asked my office to review whether or not it was appropriate. The IPC found that the third party consultation was both appropriate and necessary and that the extension of time was, therefore, appropriate. No recommendations were made.



REVIEW RECOMMENDATION 16-149

Category of Review:	Privacy Complaint
Public Body Involved:	Education, Culture and Employment
Sections of the Act Applied:	Section 59(2), Section 42, Section 47.1,
Outcome:	Recommendation mostly accepted

The Complainant had a history of migrains which sometimes made him faint. He wanted to ensure the safety officer in the office knew what to do if that happened and asked a manager to identify the safety officer in the office so he could do so. Rather than simply identifying the safety officer, the manager declared the matter a “health and safety issue” and called a full staff meeting in which the Complainant was asked to explain to the entire group the nature of his medical condition, which he did only because he felt compelled, in the circumstances, to do so. In giving his co-workers information about his condition, he compared the condition, neurologically, to a small seizure. One or more of his co-workers interpreted this to mean that the Complainant suffered from epilepsy. After the meeting, the Complainant was told he was required to tell a co-worker when he went to the washroom, who was tasked with going to look for him if he took more than five minutes. The next day, the Complainant obtained a medical note from his physician stating that he should be off work indefinitely for an unspecified medical reason. When provided with this note, the Complainant’s supervisor requested that the Complainant obtain a medical prognosis. The request for this prognosis included a reference to the Complainant's "epileptic seizures" which the letter suggested were "episodic and brief".

I requested an explanation from the public body about these allegations on February 22nd. On March 17th, the Deputy Minister advised that the department was conducting an internal investigation and that, rather than do two separate investigations, they suggested that they simply provide me with a copy of their internal review document,



when complete. When nothing further was heard from the department, additional letters were written in May, and twice in June asking for the report. On July 8th, a letter was received from the Deputy Minister indicating that their investigation would not be completed until July 28th. On August 19th, having still not received anything further from the Department, another letter was sent to them indicating that in the absence of any input from them, my office would be completing a report and making recommendations based solely on the information received from the Complainant. Very soon after having emailed this letter to the department, our office received a letter in which the Department indicated that they had completed their investigation and that the parties had been informed separately as to the outcome. The letter further indicated that it was reviewing its processes with respect to how it handles similar situations in the future to ensure awareness and compliance with privacy legislation. No explanation or other submissions were included.

With nothing from the public body, the IPC accepted the Complainant's version of events and found that there had been a serious breach of the Complainant's privacy when he was compelled to reveal personal health information to his co-workers in an open meeting,. Several recommendations were made, including a formal apology to the Complainant, and the establishment of clear written policies for managers and supervisors with respect to the collection, use and disclosure of personal health information about employees, emphasizing that personal health issues of any one employee does not constitute a "health and safety issue" that requires the sharing of information. Additional recommendations were made with respect to the Department's failure to comply with the requirements of the *Access to Information and Protection of Privacy Act*.



REVIEW RECOMMENDATION 16-150

Category of Review:	Access to Information - Fee Assessment
Public Body Involved:	Stanton Territorial Health Authority
Sections of the Act Applied:	Section 5(3), Section 50, Regulation 10, Schedule B of the Regulations
Outcome:	Recommendations Accepted Except with respect to suggested time frames

The Applicant sought copies of a series of records from the Stanton Territorial Health Authority. The public body identified 2078 responsive records and provided the Applicant with a fee estimate of \$1,262.00. The Applicant sought a review of the fees assessed. The IPC reviewed the fee assessed and found that for the most part the fee was appropriate. She noted, however, that the regulations prohibited any fee for time spent reviewing and redacting a file for disclosure and reduced the fee by \$468.00 accordingly.

REVIEW RECOMMENDATION 16-151

Category of Review:	Privacy Complaint
Public Body Involved:	Education, Culture and Employment
Sections of the Act Applied:	Section 40, Section 41
Outcome:	Recommendations accepted in part

A request was received from a member of the public to review the amount of information being collected about and from individuals receiving Income Assistance. The focus of the request was the insistence that the person applying for income assistance provide a full copy of the "Notice of Assessment" received from Revenue Canada each year. The Complainant argued that there is far more information on the Notice of Assessment than was necessary to evaluate his entitlement to income assistance. The department conceded during the review process that there was information on the Notice of Assessment that had no bearing on an individual's entitlement to assistance.



The IPC recommended that, when collecting Notices of Assessment, the Department ensure that all financial information on the document be redacted but for the numbers on lines 150 and 482. She further recommended that personal information be collected, where possible, directly from the client, even when it might be perceived as “easier” to collect the information from Revenue Canada. Finally, she recommended that when information is collected from a third party, the individual be informed about the collection, including the details of the information collected.

REVIEW RECOMMENDATION 16-152

Category of Review:	Access to Information - Extension of Time
Public Body Involved:	Sahtu Health and Social Services Authority
Sections of the Act Applied:	Section 8(1), Section 11
Outcome:	Recommendations Accepted

The Applicant requested specific and narrowly focused information from the Sahtu Health and Social Services Authority. The public body acknowledged the request and asked for clarification fairly quickly. Four days before the end of the response was due, the Applicant received notice pursuant to section 11(1)(c) extending the time for the response for 26 days so that the public body could consult with another public body. No further explanation was provided.

During the review process, the public body advised that the required consultation was taking place with the Department of Human Resources, who had received a similar request from the Applicant.

The IPC found that the public body had not established any reasonable explanation for their stated need to consult with another public body before responding and that the extension of time was, therefore, not properly taken. By the time the review was completed, however, the response had been provided to the Applicant and any specific recommendations would, therefore, be moot. The review did, however, recommend



that all public bodies make every reasonable effort to respond to all access to information requests within the initial 30 days and that the need for any consultations be identified early in the process.

REVIEW RECOMMENDATION 16-153

Category of Review: Access to Information
Public Body Involved: Sahtu Health and Social Services Authority
Sections of the Act Applied: Section 23(2)(f), 23(2)(h)(ii), 23(2)(d), 14(1)(a), 24(1)(a)
Outcome: Recommendations mostly accepted

The Applicant sought records about himself excluding information in his personnel file. When the response was received, it included only information from his personnel file and very little else. The Applicant had expected more, including hand written notes and phone call records. The Applicant requested a review with respect to the adequacy of the search, as well as with respect to the exceptions applied to the records disclosed.

The IPC commented on the practice of asking employees to search their own files to find records responsive to an access to information request, particularly when, as in this case, there seemed to be some kind of dispute between the Applicant and those from whom he was seeking records. Issues were also raised about the classification of “transitory records” and what constitutes a transitory record.

The IPC recommended the NTHSSA develop a way to verify responses received from individual employees searching their own records. She further recommended that a further search be undertaken of the email records of those employees who were in relevant positions during the time frame in question, but who were no longer employees at the time of the request for information. A number of recommendations were also made with respect to the application of exceptions in those records which were disclosed.



REVIEW RECOMMENDATION 16-154

Category of Review:	Access to Information - Deemed Refusal/Delays
Public Body Involved:	Northwest Territories Health and Social Services Authority
Sections of the Act Applied:	Section 8, Section 12,
Outcome:	Recommendation that ATIPP issues be made a priority accepted Recommendation to have a dedicated ATIPP Co-ordinator in each region not accepted, but willingness to discuss other options

A request was made to the Department of Finance (Human Resources) for access to personal information of the Applicant. Part of the request was transferred to the health authority with which he had been employed. The health authority failed to respond and the Applicant sought a review based on a deemed refusal.

The IPC noted that the Request for Information had been made commensurate with the amalgamation of six regional health and social services authorities and recognized that this probably resulted in the failure to respond to both the Applicant and to inquiries from her office. She pointed out, however, that ATIPP imposed statutory duties on public bodies and that general disorganization was not an adequate excuse for ignoring

those duties. The IPC recommended that the Northwest Territories Health and Social Services Authority take the time, as a priority, to set out thorough and clear policies and procedures with respect to the handling of access to information requests, including ensuring that there is at least one person in each of the regions who will be responsible for access to information and privacy issues under both the *Access to Information and Protection of Privacy Act* and the *Health Information Act*.



REVIEW RECOMMENDATION 16-155

Category of Review:	Privacy Complaint
Public Body Involved:	Department of Lands
Sections of the Act Applied:	Section 48
Outcome:	No recommendations made

This matter came to my attention in the form of a complaint by an employee that his supervisor had inappropriately disclosed his personal information, including personal health information, to his fellow employees. The Complainant had a doctor's note requiring him to be off work for a little over a week. When he gave the note to his supervisor, she called the Complainant's work group to a meeting at which she not only disclosed why the Complainant would be off work, but also that she had previously denied the Complainant those same days off, implying that his medical issues were not genuine. During the course of the IPC's review of the matter, the Department acknowledged that there had been a breach of the Complainant's privacy and that senior staff was likely not well educated about what constitutes personal information and how much information could be disclosed in the management of personnel. The department indicated that it had, as a result of this review, taken steps to request training options for the staff in this regard.

REVIEW RECOMMENDATION 17-156

Category of Review:	Privacy Complaint
Public Body Involved:	Department of Justice - Legal Aid
Sections of the Act Applied:	Section 40
Outcome:	Recommendations Accepted

The Complainant was an employee of a public body. He was also a parent of a young child. His child became ill and he sent his supervisor an email requesting leave for four days so that he could be home with his sick child. A medical certificate was attached to the email. This medical certificate named the child, and referred to the child's Health



Care number. It also indicated that the employee would not be able to attend work/school due to his "son's medical condition" for four days. The certificate was in a form generally accepted by the GNWT for medical absences and was signed by a physician. The next morning the Complainant received an email from his employer requesting further information about the nature of his son's illness before his special leave would be approved.

During the review process, the public body confirmed that the Complainant's supervisor over-stepped when he attempted to collect information about the nature of the child's illness. The supervisor indicated that he had received labour relations training which suggested that leave requests resulting in an operational impact on the program area required further substantiation.

The IPC recommended that the labour relations training program be reviewed to ensure that it properly addressed this issue. She further recommended that the written policies and procedures surrounding the grant of special leave be reviewed and updated so as to provide clearer guidance for what is required to approve special leave when being requested to care for a family member.

REVIEW RECOMMENDATION 17-157

Category of Review:	Access to Information - Deemed Refusal
Public Body Involved:	Aurora College
Sections of the Act Applied:	Section 6, Section 7, Section 8, Section 11, Section 26, Section 23(2)
Outcome:	Recommendations Accepted

This matter arose as a result of an application for access to certain personal information about the Applicant's employment. Job action had been taken against the Applicant and he sought access to records in relation to that job action. The public body had determined that a third party consultation was necessary and had extended the response date accordingly. After the consultation had begun, the Applicant entered into



negotiations with the public body to resolve outstanding issues. As a part of those negotiations, the Applicant agreed that the formal ATIPP process would be suspended and would be dealt with as part of the negotiations. Negotiations broke down. The Applicant gave notice that he expected a response to his Request for Information. When no immediate response was received, he sought a review by my office on the basis of a deemed refusal.

There were 6 pages of responsive records which, at the time the review began, had not been redacted for the purpose of responding to the Applicant's request. They advised, however, that before disclosing the records, some information would have to be redacted pursuant to section 23 (unreasonable invasion of a third party's privacy).

The IPC recommended the disclosure of all six pages with specific redactions pursuant to section 23. She also made recommendations about the establishment of policies to deal with instances in which the parties agree to remove a request from the formal ATIPP process under the Act, including guidelines around when such an agreement can be made, a formal process for entering into such an agreement, a policy for what happens if the agreement fails and creating time lines for the completion of the production of records in such circumstances.

REVIEW RECOMMENDATION 17-158

Category of Review:	Privacy Complaint
Public Body Involved:	Aurora College
Sections of the Act Applied:	Section 42, Section 47.1, Section 43, Section 48
Outcome:	Recommendations Accepted

The Complainant raised issues about the use/disclosure of his personal information by his former employer after his employment with the organization ended. In particular, he complained:




1. that his former supervisor had disclosed the circumstances of his departure to a number of third parties;
2. that the public body had used his signature to process cheques after his departure; and
3. that the public body had failed to shut down his email account after his departure and that one or more people within the organization were given access to the email account (including any personal email sent to that account).

The IPC found that the actions of the public body in relation to the first two complaints did not amount to a breach of privacy in that the employer was simply taking steps to ensure that the projects being worked on by the Complainant at the time of his departure were not negatively affected. The IPC found that at no time was anyone provided with any details about the Complainant's departure, simply that he was no longer working with the public body. Further, the Complainant had signed off of the cheque run on which his signature appeared before his departure and that there was no breach of privacy involved.

The IPC did find, however, that the failure of the public body to decommission the Complainant's email address after his departure constituted a breach of the privacy of not only the Complainant, but also of others who sent emails to that address not knowing that someone other than the complainant was receiving them. She found that a public body email address is an identifier attached to a person's name and that the email address assigned to the Complainant during his employment with the public body was his personal information, even though the address itself belongs to the public body. As such, keeping that email active means that there was an ongoing breach of the privacy of not only the Complainant, but potentially of third parties communicating with that email address thinking that the person reading the correspondence is the identified person. She found that six months is far too long to allow an email address to remain active after an individual is no longer an employee of the public body.



The IPC recommended a thorough review of the public body's policies and procedures with respect to the establishment, management and decommissioning of email accounts.



ARGUING THAT YOU DON'T CARE ABOUT THE
RIGHT TO PRIVACY BECAUSE YOU HAVE NOTHING
TO HIDE IS NO DIFFERENT THAN SAYING THAT
YOU DON'T CARE ABOUT FREE SPEECH BECAUSE
YOU HAVE NOTHING TO SAY.

EDWARD SNOWDON



REVIEW RECOMMENDATION 17-159

Category of Review:	Access to Information
Public Body Involved:	Department of Human Resources
Sections of the Act Applied:	Section 1, Section 6, Section 7(1),
Outcome:	No Recommendations Made

A request was made to the Department of Human Resources for copies of certain information about the Applicant's employment, in particular information from his personnel file or in relation to his employment status. Two records were identified as being responsive. The Applicant was not satisfied and felt there should be additional records.

After receiving a detailed explanation from the public body outlining the searches conducted for responsive records, the IPC found that the search was adequate and that there was nothing from which she could infer that there might be additional records that were not disclosed. Section 7, she noted, required public bodies to make a "reasonable" effort to identify and disclose responsive records. She was satisfied in this case that that was done.

ANY RESPONSIBLE ORGANIZATION THAT'S DEALING WITH INFORMATION HAS TO ASSUME THAT THEIR DEVICES ARE GOING TO GET LOST, SO THEY BETTER BE ENCRYPTED. IF YOU WANT TO PUT YOUR OWN STUFF AT RISK, FINE. BUT IF YOU'RE DEALING WITH OTHER PEOPLE'S INFORMATION, YOU REALLY HAVE AN OBLIGATION - AND THE LEGISLATION SAYS YOU HAVE AN OBLIGATION - TO TAKE REASONABLE CARE OF THE INFORMATION

Frank Work, Former Information and Privacy Commissioner, Alberta



HEALTH INFORMATION ACT

REVIEW 16-HIA01

Category of Review: Privacy Complaint
Health Information Custodian: Yellowknife Health and Social Services Authority
Sections of the Act Applied: Section 2, Section 8, Section 14, Section 15(1), Section 15(2), Section 17, Section 18, Section 22(2), Section 22(3), Section 23

Outcome:

This privacy complaint was received on October 1st, 2015, the day that the *Health Information Act* came into effect from a Complainant had had ongoing struggles with Yellowknife Health and Social Services Authority (YHSSA) over his ability to control access to his health information. His complaint was premature in that he had not had any contact with the health system since the coming into effect of the Act. This notwithstanding, the IPC proceeded with the review with a view to providing direction. The complaint dealt, generally, with two issues - the first being the conditions necessary for physicians to rely on implied consent for the collection, use and disclosure of personal health information (PHI) and the second about the patient's right to limit who can have access to his/her PHI.

Many of the concerns raised by the Complainant stemmed from the fact that there is only one service provider for primary health care in Yellowknife and, indeed, in the Northwest Territories which gives the patient no choice of health care providers. All primary health services are provided by "teams" as opposed to assigning one patient to one physician. Additionally, all of the staff of any given health facility have access to the medical health records of all patients who attend the facility, subject only to the limitations set by the roles based access to the electronic records.

Prior to the coming into force of the *Health Information Act*, the Complainant had provided YHSSA with a "personal directive" which prohibited the sharing or exchange of his personal health information without his express consent, for any reason other than for testing or emergency services. The directive further emphasized that three specific



physicians were not to have any access to his personal health information, either verbally or in written form, up to and including appointment bookings. Yellowknife Health and Social Services Authority had a difficult time complying with the directive both before and after the coming into force of the *Health Information Act*.

On the consent issue, after reviewing the many provisions of the *Health Information Act* which address the consent issue, the IPC found:

- a) consent of any kind (implied, assumed, or explicit) is not a valid consent if it is not knowledgeable;
- b) in order for consent to be knowledgeable, the custodian must inform the patient how the information will be collected, used and disclosed AND post relevant information about collection, use and disclosure in a prominent place or give notice to the individual describing the purposes of the collection, use or disclosure.
- c) the consent must not be obtained through deception or coercion
- d) the patient must know that he has the right to withhold consent

She further found that the health information custodian had not taken the steps necessary to allow them to rely on the Complainant's implied consent either before or since the coming into force of the *Health Information Act*.

On the consent issue, she recommended:

1. That within three months, YHSSA develop informational brochures which outline the patient's rights with respect to the collection, use and disclosure of personal health information, in as many as the official languages as possible.
2. That the brochure be provided to every patient who seeks medical care at any facility operated by the YHSSA for at least one year and be provided to all new patients of the clinic thereafter as well as being available in clinic waiting rooms.



3. That posters be developed for posting in waiting rooms and examination rooms of the all of YHSSA's clinics.
4. That materials be prepared and uploaded to YHSS's web page containing the same kind of information, in more detail than is available either on the poster or in the brochures.

On the issue of whether or not YHSSA had to comply with the Complainant's personal directive, she found that sections 22 and 23 of the *Health Information Act* provide that, even where consent to the collection, use or disclosure of PHI is given (either explicitly or implied) "conditions" may be put on that consent. These conditions may be placed at the time of the consent or after consent is provided but do not have retroactive effect. Nor can such conditions be used to:

- a) limit collection, use or disclosure that is required by the *Health Information Act* or any other Act;
- b) limit collection, use or disclosure that is for the purposes of a program established under the *Pharmacy Act* to monitor prescriptions;
- c) prohibit or restrict the recording of any information by a health information custodian that is required by law or by established standards of professional or institutional practice
- d) in any other prescribed circumstances

Other than these specific exceptions, there are no limits to the conditions that a patient can put on the collection, use or disclosure of his/her personal health information. The health information systems being used by YHSSA did not have the functional capacity to allow masking notwithstanding the legislative directive in the Act. Under the Act, health information custodians must have the ability to allow for a patient to put conditions on their consent.

On the issue of the patient's right to control who has access to his/her personal information, the IPC recommended:



- a) that YHSSA take immediate steps to ensure that its electronic medical record has the necessary functionality to comply with sections 22 and 23 of the Act, including
- i) the ability to limit access to an individual's personal health information to specific individuals, except in the case of an emergency;
 - ii) the ability to mask parts of an individual's personal health information from one or more users of the system;
 - iii) the ability to record and highlight the existence of conditions placed by a patient around the collection, viewing, use and disclosure of personal health information.
- b) that YHSSA take immediate steps to establish written policies and procedures with to allow patients to place conditions on the collection, use and disclosure of personal health information, including steps on how and by whom the patient will be provided with information about the implications of such conditions.
- c) that immediate steps be taken to ensure that the conditions set out in the Complainant's "personal directive" be recorded, implemented and honoured in accordance with the *Health Information Act*;

REVIEW 16-HIA02

Category of Review:	Privacy Complaint
Health Information Custodian:	Yellowknife Health and Social Services Authority
Sections of the Act Applied:	Section 8, Section 9(2), Section 10,
Outcome:	Recommendations partially accepted

The Complainant was staying at a medical boarding home for the purpose of completing a sleep study. The sleep study was done by a private sector company under contract with the STHA to conduct sleep studies. This company had been provided with some basic health information about the patient including the patient's name, date of birth, health care number, a brief medical history, the reason for the referral, current medications, height and weight. In this case, a two page physician referral letter was also provided. The study was conducted at the medical boarding home. The day



following the testing, the Complainant says he found his referral paperwork on the front desk of the boarding home, where anyone could see it. He contacted STHA about the breach.

The contractor doing the study admitted that its employee had misplaced the referral documents.

The IPC found that the company conducting the sleep study was an “agent” of the STHA and that it was, therefore, the responsibility of the STHA to ensure appropriate protections for the privacy of the patient. It is not sufficient to simply rely on confidentiality clauses in contracts. She made the following recommendations:

- a) that the STHA or the NWTHA, as the case may be, immediately start the process of creating and implementing written standards, policies and procedures to ensure compliance with Section 8 of the *Health Information Act*,
- b) that the STHA or the NWTHA, as the case may be, review all of its contracts with third parties, particularly those in the private sector, and amend those contracts so as to include clear and specific obligations for those third party agents with respect to the collection, use, disclosure, security and disposal of personal health information and that any new contracts include such provisions.
- c) that within three months, the STHA or the NWTHA, as the case may be, develop stepped informational materials which address:
 - how and in what circumstances a patient's personal health information may be collected, uses and disclosed;
 - information about the use of electronic records and how access to records is controlled within the electronic record system;
 - information about the "team" approach to medical care and how that affects the use of personal health information
 - the right of patients to place conditions or limits on how their personal health information is used and who has access to it;



- the contact information for someone within the organization who is available to answer questions or help the patient with placing conditions on their consent
- the right of the patient to find out who has had access to their electronic medical record and to request that an audit be done.

REVIEW 16-HIA03

Category of Review: Breach Notification
Health Information Custodian: Beaufort-Delta Health and Social Services Authority
Sections of the Act Applied: Section 86, Section 87, Section 137
Outcome:

This review was initiated as a result of a notification received from the Beaufort-Delta Health and Social Services Authority (BDHSSA) pursuant to section 87 of the *Health Information Act*. The notice informed the IPC that the authority had uncovered repeated inappropriate viewing of patient information by clinic staff using the electronic MediPatient system at the Inuvik Regional Hospital.

The breaches were discovered as a result of a complaint made to the CEO of the Inuvik Regional Hospital by a patient. The patient indicated that a Clerk at the clinic in the Inuvik Regional Hospital had accessed the patient's information in the MediPatient system and conducted an unwelcome visit to the patient while he was hospitalized. The unauthorized access to the MediPatient system was confirmed by the health authority after conducting an investigation which included interviewing witnesses and conducting an audit of the employee's use of the system. The investigation found that the clerk in question had accessed the inpatient bed history many hundreds of times, mostly after 5:00 pm, during lunch breaks, coffee breaks and during walk-in clinics. They also found that the clerk had accessed individual patient records multiple times a day or multiple times during a particular patient's stay in hospital. As a result of this initial investigation, and the seriousness of the breach, BDHSSA did a wider investigation to determine whether this kind activity was prevalent throughout the hospital or if it was contained to the one employee or the one department. This wider investigation found that six staff



members within the clinic had very likely been breaching patient privacy on a regular or semi-regular basis and that there appeared to be a "culture of inappropriately accessing patient information" within the clinic. One staff member was terminated and the others suspended with pay for a period of time. BDHSSA took steps to notify all patients they could identify as being affected by the breaches. The investigation also showed, however, that the snooping was limited to the clinic and there was no evidence that it was pervasive throughout the Authority.

After BDHSSA had completed its internal review, they asked to meet with me to discuss the results. After that meeting, I provided them with notice that I would be undertaking a review pursuant to section 137(1) of the *Health Information Act*. The IPC accepted the BDHSSA's investigation as the basis of her report and made comment about a number of issues that needed to be addressed, including the way in which access to the medical health record was administered, the sharing of passwords and log-ins, poor administration of the password system, the absence of any employee who had a good understanding of functionality of the electronic record system, and a lack of appropriate orientation and leadership.

The IPC made a number of recommendations, including:

- a) that NTHSSA establish a full time position of Privacy Officer in each of its regions with the specific responsibilities and attributes and that these positions be properly funded and supported in order to ensure that the incumbent is able to do an effective job.
- b) that the MediPatient be reconfigured or changed so that it is more effective in protecting itself including:
 - i) having the system itself generate unique passwords for each new user;
 - ii) requiring a new password to be confirmed and/or changed with a certain time period, failing which access to the system is denied;
 - iii) having the system periodically remind users to change their passwords and shut them out of the system until they do so;



- c) having the system disallow the use of the same password by more than one user;
- d) ensuring that all employees are currently using unique passwords and emphasizing that passwords are not to be shared for any reason, with appropriate consequences if this rule is breached, up to and including termination of employment;
- e) prohibiting or restricting access to any electronic record by new employees until they have demonstrated an understanding of their basic responsibilities with respect to the collection, use and disclosure of personal health information;
- f) informing employees that they will be held responsible for all activity under their user name and that if they do not close their systems when they walk away from their desks, they may be held responsible for another employee's actions, whether or not they are actually guilty of inappropriate use or disclosure of information on the system, coupled with a warning about the penalties under Part 8 of the *Health Information Act*;
- g) conducting regular audits on the use of the MediPatient system, focused both on "suspicious" activity and random audits of individual employees to test how they are using the information on the system
- h) giving priority to identifying the specific access required for each position within the regional health system and ensuring that all electronic health record systems are configured so as to restrict access to only the information needed for each employee to do his or her job;
- i) configuring the MediPatient system so as to send up clear on-screen warnings when a user is accessing or attempting to access information beyond that which they have been given access and to flag such attempts as well as other "suspicious" behavior.



EMERGING ISSUES

The Northwest Territories is one of the last jurisdictions to take a close look at its first generation Access and Privacy legislation with a view to making changes to meet the needs of the modern technological world we live in. This allows us to learn from others and to gather the best from around the country. There is much work being done in this arena and it is important that the Northwest Territories keep pace. I am hopeful, based on my discussions with Department of Justice officials working on the review of the Act, that we will be presented with modern and even a forward looking new legislation in the coming months. This said, not everything is about the legislation. Good access and privacy also require strong leadership, good policies, and good information management.

Good Information Management Practices and Policies

When the ATIPP Act came into force, most record keeping was still paper based and there were strong information management professionals in most, if not all, government agencies to ensure that those records were properly classified, stored and archived so as to preserve the historical record of decision making by government. Over the last twenty years, however, this kind of information management has gone the way of the dodo, and every employee is now expected to manage their own records. There are still policies and procedures with respect to file management, but little is done to ensure that employees are knowledgeable about and applying good information management practices. Every employee with a computer has control over his or her record keeping system, which leads to uneven records management. There is a direct relationship between good records and information management and the ability of a public body to meet its responsibilities under either the *Access to Information and Protection of Privacy Act* or the *Health Information Act*. Good records and information management practices can prevent records from being lost or misfiled, or from being improperly deleted. At the same time strong records and information management practices will reduce the time and effort required to identify and gather records in response to an access request. More resources and focus need to be committed to this basic function of government - good, consistent and monitored record keeping.



The Use of Instant Messaging and Personal Devices for Business

Many public servants and elected officials use communications tools such as texts, instant messaging and web-based personal email accounts to assist them in the work that they do. While this may be a current day reality, it is also bad practice which not only threatens the ability of the public to gain access to government records but also is a considerable threat to privacy. While it may be difficult, perhaps impossible, in today's world, to prohibit the use of such tools by GNWT employees, there needs to be more done to limit the use of communications tools outside of the GNWT system and to provide clear guidance on proper procedures when such forms of communication are used. The Northwest Territories is certainly not alone in dealing with this reality. The Information and Privacy Commissioner of Ontario published a guidance document in June of 2016 that addresses this issue which provides direction and advice on this issue which can be found at <https://www.ipc.on.ca/wp-content/uploads/2016/08/Instant-Messaging.pdf>.

I encourage all departments and other public bodies to make this required reading for all employees.

Communicating Personal Health Information

The *Health Information Act* requires that health information custodians protect the personal health information of their patients. The reality of our health system is that information has to flow to provide effective services. When it comes time to move health information from one place to another, however, it seems that the sector appears reluctant to embrace the technology designed to protect information. In particular, I continue to receive a significant number of breach notifications about misdirected faxes. Fax technology is now old technology and should be used only in exceptional circumstances. While all means of transferring information from one place to another have inherent risks, it is much easier to mitigate those risks in the digital arena. Emails can be encrypted to protect the content so that, in the fairly likely event that an email goes astray from time to time, the content is not disclosed.

Unfortunately, it also appears that the use of encryption technology in the NWT health sector is not prevalent. As a result, there have also been reports of misdirected emails of personal health information resulting in breaches of privacy.



More energy and attention needs to be focused on how information is communicated from place to place within the system so as to avoid potential breaches. Encrypted email is likely the easiest and most effective way to do this. Health information custodians need to make this the mandatory method of communications except in situations which makes this impossible or the urgency of the situation makes it infeasible.

Disclosure of Personal Information in the Workplace

I received two very similar complaints this year from GNWT employees whose personal information was disclosed to co-workers by supervisors or managers in a very public way. In each case, the information was disclosed in a meeting of the entire work group, called by a manager specifically for the purpose of discussing an employee's personal circumstances. In both cases, personal health information about an employee was disclosed without the consent of the employee. In neither case was there any operational need or justification for the disclosures made in these meetings.

What I take from these two incidents is that managers need to be more educated about privacy in the workplace. In both cases I recommended that supervisors and managers receive more ATIPP training. I make this same recommendation for all public bodies.

Breach Notification

More and more Canadian jurisdictions are moving toward a requirement of mandatory breach notification where there has been a material breach of privacy or where there is a real risk of significant harm as a result of a privacy breach. With the *Health Information Act*, the Northwest Territories now has mandatory breach notification in the health sector. With these provisions, we can start to see with some clarity how personal information can go astray and focus on how to fix the holes that allow this to happen. Requiring public bodies to identify and track breaches of privacy requires public bodies to focus on their policies and procedures, I am hoping that mandatory breach notification for all public bodies will be included in the coming amendments to the Act, in the meantime I would very much like to see this start on a voluntary basis.

Adequate Resources

Even perfect legislation will fail if there are inadequate resources to meet the demand. This year has demonstrated, even more than in previous years, the need for more resources to be dedicated to access and privacy, both within public bodies and in my office. A number of public



bodies have been struggling to keep up with access to information requests and the resulting Requests for Review. The amalgamation of six health and social services authorities in August of last year, combined with a large turnover of senior staff resulted in a complete breakdown of the processes related to access to information. For a period of nearly six months, responses from any of the amalgamated health authorities were virtually non-existent. While this issue appears to be resolving itself, it has been a difficult transition in terms of access and privacy, perhaps made more so as a result of the coming into force of the *Health Information Act* less than a year before the transition.

But the health system is not alone in its struggles. Both the Department of Human Resources and Aurora College have struggled to meet their responsibilities under the *Access to Information and Protection of Privacy Act*. Both of these public bodies have received an unprecedented number of Access to Information requests and been the subject of a number of privacy complaints. ATIPP is a client driven function of government. There is a very real ebb and flow to the volume of work as a result. That said, when the tide is high, public bodies need to have the resources and the flexibility to deal with whatever comes in the door.

As noted earlier in this report, my office is also struggling to keep up. With a 40% increase in case load in one year and the promise of an even more dramatic increases in work load into the 2017/2018 fiscal year, one person simply cannot keep up with the demand. Last year, I asked for an increase in my budget to allow me to expand the staff contingent in the office with an Assistant Commissioner/Investigator. That request was denied. I renew that request this year. Without the additional manpower, my ability to keep up with the ever increasing demands of the office will continue to deteriorate. Freedom of Information and protection of privacy legislation has been held by Canada's Supreme Court to be quasi-constitutional in nature. It is important that the necessary resources are committed to the work mandated by the legislation.





**OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER**

NORTHWEST TERRITORIES

Rapport annuel 2016-2017

LOI SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DE LA VIE PRIVÉE
LOI SUR LES RENSEIGNEMENTS SUR LA SANTÉ





MESSAGE DE LA COMMISSAIRE

L'année 2017 marque ma 20^e année à titre de commissaire à l'information et à la protection de la vie privée des Territoires du Nord-Ouest, et le 20^e anniversaire de l'entrée en vigueur de la *Loi sur l'accès à l'information et la protection de la vie privée*. La nature de mon travail a beaucoup évolué depuis 1997. Quand j'ai commencé, tout tournait autour de « l'accès à l'information ». Au fil des ans, la

technologie a évolué et la valeur des renseignements personnels s'est accrue, si bien que la « protection de la vie privée » est devenue l'une de nos principales préoccupations. Au cours des dernières années, toutefois, l'aspect « accès à l'information » a été ramené au premier plan, et cela semble être la tendance à la grandeur du pays. Si la population se soucie toujours de la capacité des gouvernements à protéger les renseignements qu'ils recueillent, on peut expliquer le regain d'intérêt pour « l'accès à l'information » par des changements dans les réalités politiques, l'augmentation de la valeur de l'information et le fait que le grand public exige plus que jamais que les gouvernements agissent de façon transparente et responsable. Comme l'indique mon homologue de la Nouvelle-Écosse dans son rapport annuel 2016-2017 :

Le monde a beaucoup changé au cours des vingt-quatre dernières années. En 1993, il n'y avait que 130 sites Web. Aujourd'hui, il y en a un milliard. Google n'a été fondée qu'en 1998 et Facebook, en 2004. Seuls les scientifiques et les rêveurs envisageaient le concept de « mégadonnées ».



Dans ce monde dont personne n'aurait pu prévoir l'évolution en 1997, une chose demeure certaine : des lois solides en matière d'accès à l'information et de protection de la vie privée sont essentielles au maintien de nos idéaux démocratiques.

Cette année, j'ai effectué mes trois premières révisions en vertu de la nouvelle *Loi sur les renseignements sur la santé*. Deux d'entre elles visaient des plaintes pour atteinte à la vie privée, et la troisième découlait d'un avis en vertu de l'article 87. Au fil de ces révisions, la loi m'est apparue dans toute sa complexité; elle est dense et difficile à interpréter, et il s'ensuit que ces révisions sont plus laborieuses et chronophages que le sont celles du même genre faites en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*. Il est à espérer que le temps requis pour chaque révision ira en diminuant au fur et à mesure que nous nous familiariserons avec la loi et son interprétation. La conclusion de chacune de mes révisions est que les dépositaires de renseignements sur la santé dans le secteur public sont loin de se conformer à la loi, et qu'il y a donc encore beaucoup de chemin à faire. La fusion de six administrations de santé régionales a créé d'énormes trous dans la capacité de la nouvelle administration territoriale à répondre aux demandes d'accès à l'information en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*. Cela dit, je commence à voir des progrès quant au respect de la *Loi sur les renseignements sur la santé* et davantage d'uniformité à la grandeur du réseau. C'est une bonne chose. Il reste néanmoins du pain sur la planche. En particulier, il semble que les systèmes électroniques utilisés par le ministère de la Santé et par l'Administration des services de la santé et des services sociaux ne permettent toujours pas aux patients de contrôler la consultation et l'utilisation de leurs renseignements, comme l'exige la nouvelle loi.

C'était encourageant de suivre le premier examen exhaustif de la *Loi sur l'accès à l'information et la protection de la vie privée* cette année, et de participer à de vastes consultations organisées avec le ministère de la Justice pour adapter la législation aux réalités d'aujourd'hui. Cet examen s'imposait depuis longtemps, et je me réjouis des efforts déployés pour rendre la loi plus fonctionnelle dans le monde moderne; c'est également très motivant de constater qu'on commence à accorder de l'importance à des idées innovantes et progressistes. J'ai bien hâte de pouvoir continuer mon travail au Ministère, qui déposera un nouveau projet de loi au cours des prochains mois.



L'augmentation rapide de la charge de travail gérée par notre commissariat témoigne de la nécessité de réviser autre chose : les ressources consacrées au Commissariat. Au cours de l'exercice 2016-2017, le nombre de dossiers ouverts à notre bureau en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* a augmenté de 40 %. En fait, notre charge de travail globale a augmenté de 157 % depuis 2013-2014^{*}. Cette tendance se maintient et tend même à s'accélérer au premier trimestre de 2017-2018. J'ai beau travailler diligemment pour dominer la situation, c'est une cause perdue. J'ai été incapable de compléter certaines révisions au cours des six mois du mandat, et le retard s'accumule d'un mois à l'autre. Je renouvelle donc ma demande d'augmenter le budget alloué au Commissariat pour que nous puissions embaucher un enquêteur et commissaire adjoint et continuer d'accomplir notre mandat tel qu'il est prescrit par la loi.

En mars dernier, j'ai sauté sur l'occasion de participer à la conférence internationale « *Transparence pour le XXI^e siècle* », organisée à Ottawa par la commissaire à l'information du Canada. Différents thèmes ont été abordés, comme les perspectives internationales sur le droit à l'information, le rôle du quatrième pouvoir et les droits des peuples autochtones. J'ai aussi continué de participer au forum pancanadien d'Inforoute Santé du Canada, qui s'intéresse depuis des années au respect de la vie privée dans le secteur de la santé. Enfin, à l'invitation du commissaire à la protection de la vie privée du Canada, j'ai aussi pris part à une rencontre organisée par son Commissariat pour discuter des concepts de « *consentement* » et de confidentialité dans ce monde interconnecté. Toutes ces conférences et rencontres ont été formatrices et intéressantes. Pour moi, toutefois, la rencontre la plus importante est, chaque année, la réunion annuelle avec mes homologues fédéraux, provinciaux et territoriaux. Celle de cette année a eu lieu en Ontario. Nous avons parlé d'une foule de sujets : les divulgations faites dans l'intérêt du public, les défis posés par les changements gouvernementaux, l'examen pancanadien des développements en matière d'accès et de confidentialité, la transparence gouvernementale, ainsi que la surveillance et les mégadonnées.

^{*} 30 dossiers ouverts en 2013-2014; 69 en vertu de la LAIPVP plus 8 en vertu de la LRS en 2016-2017.



J'ai aussi eu le plaisir, cette année, de cosigner un mémoire à l'occasion de la consultation publique sur la modernisation du cadre de sécurité nationale. La préparation de ce mémoire a été dirigée par le Commissariat à la protection de la vie privée du Canada, et tous mes homologues provinciaux et territoriaux ont signé le document. Ce mémoire s'attaque à plusieurs dossiers ayant notamment trait au partage de renseignements à l'échelle nationale et internationale, à la collecte et à la conservation de métadonnées liées aux communications, à l'accroissement de la transparence et de la surveillance des agences impliquées dans la sécurité nationale, et aux propositions visant à faciliter l'accès aux renseignements sur les abonnés et aux communications chiffrées pour les forces de l'ordre.

En terminant, j'aimerais remercier chaleureusement mon assistante, Lisa Phypers. Sa rigueur, son dévouement, sa persévérance et sa bonne humeur facilitent grandement mon travail.



BILAN DE L'ANNÉE

Dans l'ensemble

Le Commissariat à l'information et à la protection de la vie privée a ouvert un total de 69 dossiers en 2016-2017, ce qui représente une augmentation de 40 % par rapport à l'exercice précédent. C'est sans compter les 42 nouveaux dossiers au Nunavut, qui représentent une augmentation de 25 % pour ce territoire. Au cours de la moitié du premier trimestre de l'exercice 2017-2018, on compte 24 nouveaux dossiers aux Territoires du Nord-Ouest et 15 au Nunavut. Il va sans dire que les ressources de l'unique personne qui s'occupe de ces deux territoires sont loin de suffire. Résultat? Les requérants sont soumis à des retards considérables, et les 180 jours mentionnés au paragraphe 31(3) sont souvent largement dépassés avant que la commissaire soit en mesure de terminer son rapport et de formuler ses recommandations. Cette augmentation du nombre de demandes n'a pas de quoi surprendre. En effet, le Nord suit la même tendance qu'ailleurs au Canada; partout, la vie privée et l'accès à l'information soulèvent plus d'inquiétudes que jamais, et les citoyens se manifestent davantage auprès de leurs gouvernements.



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

Le Commissariat a ouvert 61 dossiers en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* en 2016-2017, comparativement à 43 au cours de l'exercice précédent. Les dossiers ouverts se répartissent dans les catégories suivantes :

Accès à l'information	
Demandes de révision générales	19
Plaintes : refus présumés	7
Plaintes : prorogations de délai	4
Frais	1
Objections d'un tiers	1
Atteinte à la vie privée	
Plaintes générales	11
Avis d'atteinte à la vie privée : organismes publics	1
Avis d'atteinte à la vie privée : autres	2



Commentaires/consultations	5
Demandes diverses	7
Administration	3

Une part de cette augmentation peut être attribuée au fait que plusieurs demandes ont été reçues de la même source au cours d'un bref laps de temps – parfois, elles concernaient toutes le même organisme public. Ceci explique aussi le nombre élevé de « présomptions de refus » : certains organismes publics qui ne sont pas habitués à gérer un tel volume n'arrivent pas à répondre à la demande. Plusieurs organismes qui ont reçu en peu de temps de nombreuses demandes de renseignements n'ont pas pu clore les dossiers dans les 30 jours prescrits.

Ces chiffres suggèrent également un changement de tendance : on recommence à s'intéresser davantage à l'accès à l'information qu'à la vie privée. C'est un phénomène qu'on observe dans tout le Canada. Même si la population demeure préoccupée par le respect de la vie privée, il y a eu, au cours des derniers mois, un regain d'attention pour l'accès à l'information.

Les « demandes diverses » incluent les allocutions, les demandes d'accès incomplètes ou ne relevant pas de la compétence du Commissariat, ainsi que les dossiers traités prestement sans qu'une révision complète ait été nécessaire.

Le Commissariat a formulé quinze recommandations relatives à des demandes de révision.



Loi sur les renseignements sur la santé

La *Loi sur les renseignements sur la santé* est entrée en vigueur le 1^{er} octobre 2015. Au cours de l'exercice 2016-2017, le Commissariat a ouvert huit dossiers en vertu de cette loi :

- a) trois avis d'atteinte à la vie privée reçus de la part de diverses instances de l'Administration des services de la santé et des services sociaux des Territoires du Nord-Ouest;
- b) deux dossiers impliquant une évaluation des répercussions sur la vie privée en vertu du paragraphe 89(2) de la loi;
- c) un commentaire adressé au ministre de la Santé à propos du plan d'action sur les soins de santé mentale;
- d) deux dossiers administratifs, dont un relevant d'une discussion continue entre le Commissariat et l'Administration des services de la santé et des services sociaux à propos des problèmes ayant fait surface et des dossiers traités dans l'année.

Nous avons produit en 2016-2017 trois rapports officiels assortis de recommandations formulées en vertu de la *Loi sur les renseignements sur la santé*.

Dans mon dernier rapport annuel, j'ai été très critique à l'égard de l'incapacité du ministère de la Santé et de ses organismes à satisfaire aux nouvelles exigences de la loi, et du manque d'effort pour éduquer le public sur ses droits et responsabilités. Les choses semblent s'améliorer, quoique lentement. On a vu des progrès du côté des politiques, des procédures et des normes à appliquer dans tout le système en vertu de l'article 8. Le nombre d'avis d'atteinte à la vie privée a augmenté, ce qui laisse supposer qu'il y a une meilleure compréhension de ce qui constitue une atteinte selon la loi. De plus, ces avis sont dûment traités et des mesures sont prises pour éviter que de telles atteintes se reproduisent. Enfin, au cours des derniers mois, j'ai remarqué que certaines cliniques, à Yellowknife notamment, ont installé des affiches pour informer les patients de leurs droits fondamentaux.

Il reste toutefois de nombreuses lacunes à combler. La plus grande est que les systèmes utilisés par l'Administration des services de la santé et des services sociaux ne permettent pas encore aux patients d'exercer pleinement leurs droits en vertu de la nouvelle loi. Cette dernière leur donne clairement le droit de limiter l'accès à leurs renseignements médicaux, mais il semble qu'aucun système électronique de tenue de dossier médical en usage aux Territoires du Nord-Ouest – du moins au niveau gouvernemental – ne permette de masquer une partie ou la totalité



du dossier du patient. On ne peut pas non plus configurer les systèmes de façon à empêcher un professionnel de la santé de consulter le dossier médical d'une personne.

En dépit des améliorations constatées au cours de l'année, il reste beaucoup de travail à accomplir. La courbe d'apprentissage est abrupte, et il faudra encore un moment avant d'atteindre un respect élémentaire de la législation. On peut donc s'attendre à ce que la *Loi sur les renseignements sur la santé* génère beaucoup de travail pour le Commissariat au cours des prochaines années.

