TABLED DOCUMENT 32-17(5)
TABLED ON FEBRUARY 11, 2014

ANNUAL REPORT 2012 - 2013

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

RAPPORT ANNUEL 2012-2013

DE LA COMMISSAIRE A L'INFORMATION ET A LA PROTECTION DE LA VIE PREVEE DES TERRITOIRES DU NORD-OUEST

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

5018 - 47th Street
P.O. Box 262
Yellowknife, NT
X1A 2N2

October 31, 2013

Legislative Assembly of the
Northwest Territories
P.O. Box 1320
Yellowknife, NT
X1A 2L9

Attention: Colette Langois
Acting Clerk of the Legislative Assembly

Dear Madam:

I have the honour to submit my annual report to the Legislative Assembly of the Northwest Territories for the period from April 1st, 2012 to March 31st, 2013.

Yours very truly

Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories

/kb

In Yellowknife: 867-669-0976 ♦ Toll free: 888-521-7088 ♦ Fax: 867-920-2511 ♦ E-mail: AtippComm@theedge.ca

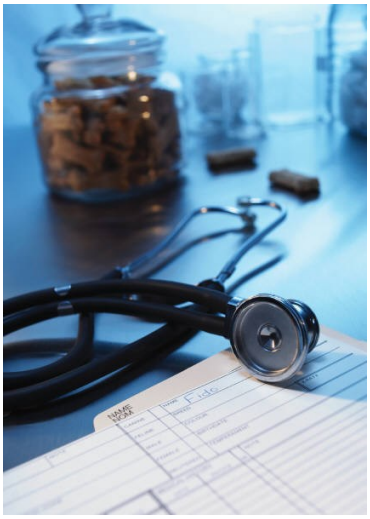
INDEX

COMMISSIONER'S MESSAGE

Looking back on fiscal 2012/2013, it has definitely been the year of health privacy concerns. Of the sixteen new files opened during the year, seven of them dealt in one way or another with health information. Of the twelve Review Recommendations completed during the year, seven of them were focused on the collection, use or disclosure of personal health information. The issues ranged from patient concerns about the way in which their personal health information was being shared within the confines of a health authority to concerns raised by patients who were also employees of one of the Northwest Territories' Health Authorities who questioned whether or not fellow employees or supervisors had access to their personal health records. And, once again, there were cases of misdirected faxes containing personal health information.

What is becoming abundantly clear from this concentration of health privacy concerns being raised is that the public is very concerned about the privacy of their personal health information. There seems to be a disconnect, in many cases, between how the public understands their information is used and disclosed within the health system and how personal health information actually flows. Further, there seems to be

a bit of a reticence on the part of health care authorities to recognize that health information is personal to the patient and that the patient is entitled to a degree of control over that information. It is, therefore, all that much more important to ensure that the proposed Health Information Act be brought forward as soon as possible for public debate and review. Furthermore, when that proposed legislation is tabled, it is important that the public be engaged in its review. For the most part, the public trusts the health system to properly protect our personal health information. But when there is a breach, it can have significant consequences to the individual. The health system is a complex one, and the exchange of information is required to provide proper treatment. This is even more pronounced in the North, where it is often necessary to travel, either within the jurisdiction or to another province, for treatment and necessary information must follow the patient. It is important that the public have confidence in the system that is being developed - that they trust that, notwithstanding the need to exchange their personal health information, their information is being used only for the purposes they understood it would be used for when collected, and that they can control who sees that information. I therefore look forward to seeing the new health privacy legislation rolled out as soon as possible. When that does happen, new resources will need to be allocated to the Office of the Information and Privacy Commissioner to deal with the added oversight responsibilities which will be created under that legislation.



While health privacy was the focus of much of my work this year, this is not the only issue of concern. I have, for several years, been advocating that the Northwest Territories do a comprehensive review of the *Access to Information and Protection of Privacy Act*. Interestingly, at the annual gathering of my counterparts from across the country in August of 2012, the Information and Privacy Commissioners of Canada unanimously passed a resolution calling on provincial/territorial and federal governments to recommit to the fundamental democratic values underpinning access and privacy legislation by consulting with the public, civil society and Information and Privacy Commissioners on how best to modernize access and privacy legislation in light of modern information technologies, evolving government practices and citizens' expectations and by modernizing and strengthening these laws in keeping with more current and progressive legislation around the world. A copy of the resolution has been appended to this Annual Report as an appendix. As noted by Elizabeth Denham, the Information and Privacy Commissioner of British Columbia in her most recent annual report:

> Unlike the private sector, where consumers largely still have a degree of choice about where and with whom they share their personal information, we do not have a choice when dealing with government. Citizens do not get to decide whether to provide personal information in exchange for health care, or services like a driver's license or passport; rather, it is a condition of entry.
>
> It is therefore imperative that public bodies implementing new information systems.....provide these services while protecting privacy. Independent oversight is vital as these programs are developed.

THE *ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT*

The *Access to Information and Protection of Privacy* (ATIPP) *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 it establishes rules about the collection, use and disclosure of information about individuals by NWT public bodies.

ATIPP applies to all "public bodies". This includes all GNWT departments, crown corporations, and some boards, commissions and agencies.

The Supreme Court of Canada has declared that laws like the ATIPP Act are special kinds of laws that define fundamental democratic rights of citizens. They are "quasi-constitutional" laws that generally are paramount to other laws.

ACCESS TO INFORMATION

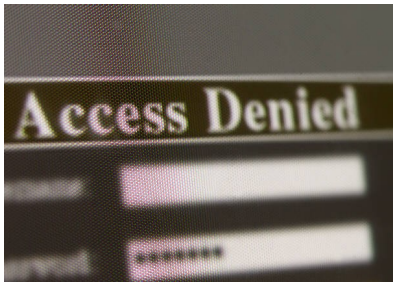
The Act provides the public with a process to obtain access to most records in the possession or control of public bodies. Generally, the public has right to any record which public bodies hold. There are, however, a number of specific and limited exceptions to this right. Most of the exceptions function to protect individual privacy rights, to allow elected representatives to research and develop policy and the government to run the "business" of government. Courts throughout Canada, up to and including the Supreme Court of Canada, have interpreted access to information legislation such that access to information is always to be considered the standard and that any exceptions applied must be narrowly interpreted so as to allow the greatest possible access to government records.

To obtain a record from a public body, a request must be made in writing and delivered to the public body from whom the information is sought.

When a request for information is received, the public body has a duty to identify all of the records which are responsive to the request. Once the responsive documents are identified, they are reviewed to determine if there are any records or parts of records which are protected from disclosure under the Act. Public bodies are required to provide a response within thirty (30) days.

If a response is not received within the time frame provided under the Act, or if the response received is not satisfactory, the applicant can ask the Information and Privacy Commissioner to review the decision made.

PROTECTION OF PRIVACY



Part II of the ATIPP 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 also provides a mechanism which allows individuals the right to see and make corrections to information about themselves in the possession of a government body.

This part of the Act also requires public bodies to maintain adequate security measures to ensure that the personal information which they collect cannot be accessed by unauthorized individuals.

THE ROLE OF THE INFORMATION AND PRIVACY COMMISSIONER

The office of the Information and Privacy Commissioner (the IPC) was created to provide independent oversight on questions that arise with respect to the application and interpretation of the Act. The IPC is appointed by the Commissioner of Northwest Territories on the recommendation of the Legislative Assembly and holds office for five year terms. As an independent officer, the IPC can be removed from office only "for cause or incapacity". This allows her to comment freely and directly.

There are four major elements in the work done by the Information and Privacy Commissioner:

1. The Commissioner responds to requests for review of decisions made by government institutions in response to access requests, and makes recommendations to those bodies.
2. The Commissioner responds to complaints from individuals who believe their privacy has not been respected by government institutions and makes recommendations to those bodies.

3. The Commissioner provides advice to government institutions on legislation, policies or practices that may impact citizens' access or privacy rights.

4. The Commissioner provides education with respect to information rights including both access to information and protection of privacy.

When issues are raised as a result of a response to a request made for access to government information, the role of the Information and Privacy Commissioner (IPC) is to provide an independent, non-partisan oversight of decisions made by public bodies.

When the Information and Privacy Commissioner receives a Request for Review, she will take steps to determine what records are involved and obtain an explanation from the public body as to how and why they came to their decision. The Applicant is also given the opportunity to provide input, as well as any third parties whose information is the subject of the request. The IPC has the benefit of being able to review, in almost every case, copies of all of the responsive records in their original format as well as in the form that they have been provided to the Applicant, showing which pages have been disclosed, which have been withheld and showing any words or paragraphs which have been redacted by the public body in responding to the request. The IPC considers the input of all interested parties, the records themselves and the provisions of the ATIPP Act and produces a report containing recommendations. The IPC generally does not have any power to compel public

bodies to either disclose or protect information from disclosure but she is required to make recommendations.

The head of the public body must make a final decision to either accept recommendations made by the IPC, reject those recommendations or take such other steps as he or she considers appropriate having considered the recommendations made by the IPC. If the person who sought the information is not satisfied with the decision made by the head of the public body, that person may apply to the Supreme Court of the Northwest Territories for a final determination of the matter.

The Information and Privacy Commissioner also has the jurisdiction to investigate and provide comments and recommendations in situations in which an individual feels this his or her personal information has been improperly collected, used or disclosed. When a privacy complaint is received, the IPC will do an investigation to determine exactly what happened, how it happened and whether or not there was a breach of the individual's privacy. Whether or not there has actually been an improper collection, use or disclosure of personal information, the IPC will prepare a report which will almost always contain comments and recommendations to improve policies and procedures so as to reduce the possibility of future breaches. The recommendations made by the IPC with respect to privacy issues are provided to the head of the public body and, once again, the head of the public body then has to decide whether or not to accept those recommendations. There is, however, no right to appeal the public body's decision respecting a privacy breach to the courts.

THE YEAR IN REVIEW

The fiscal year 2012/2013 was another busy one for the Information and Privacy Commissioner. In the 12 months between April 1, 2012 and March 31, 2013, the office opened 16 files, down slightly from the previous year. The files can be divided into a number of categories:

a)	Breach of Privacy Complaints	4
b)	Request for Review - Access to Information	1
c)	Misdirected Medical Faxes	3
d)	Delay	1
e)	Request for Review - Fee Assessment	5
f)	Found medical records	1
g)	Administrative	1

All of the Fee Assessment request were resolved through an informal process and no report or recommendations were, therefore completed. Two of the three cases that arose as a result of misdirected faxes containing personal health information were self-reported by the health authority. Because, in each of these cases, the public body had discovered the error quickly, and taken active steps to address the mistake, I chose not to do a full report on these

two reports. The file dealing with delay was resolved very quickly after I became involved and, once again, I exercised my discretion not to do a full report or make formal recommendations in this case. I did, however, provide the public body with a long letter outlining my concerns and suggestions to address the source of the delay in this case. Finally, in one instance, a member of the public brought in a piece of paper he had found in an alley in downtown Yellowknife which contained personal health information of an individual. With the information contained on the paper, I contacted the individual involved to advise him that the paper had been found and asking him if he had any concerns arising as a result. As I did not hear from him further, based on the content of the document, I concluded that the paper was most likely lost by the individual himself. There was no indication at all that the document found its way onto the street via a health care provider. I therefore chose to take no further action on this matter.

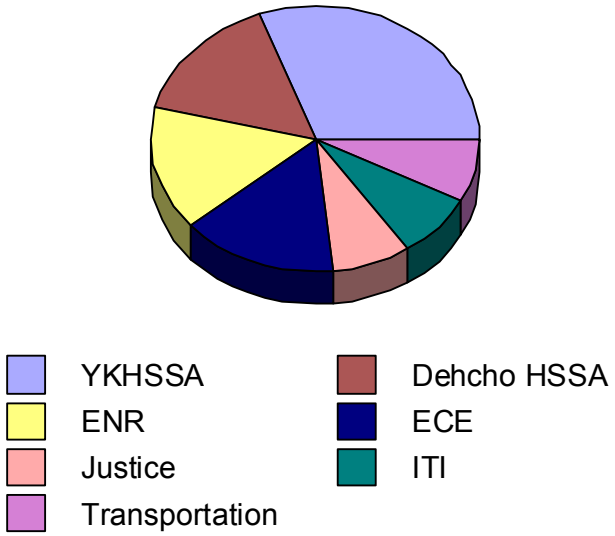
A number of public bodies were involved in the matters before me this year:

Yellowknife Health and Social Services Authority	4
Dehcho Health and Social Services Authority	2
Energy and Natural Resources	2
Education, Culture and Employment	2
Justice	1
Industry, Tourism and Investment	1

Transportation	1
Executive	1

Twelve Review Recommendations were issued by the office of the Information and Privacy Commissioner in 2012-2013.

Public Bodies Involved



REVIEW RECOMMENDATIONS

REVIEW RECOMMENDATION 12-105

A Complainant, who was also an employee, alleged that his personal health information had been improperly used or disclosed by the Beaufort-Delta Health and Social Services Authority (BDHSSA), after having received medical assistance from the health authority. He alleged that records from that medical appointment were later used, without his consent, in the context of a disciplinary proceeding involving his employment. When he asked for an explanation from the CEO about the apparent breach of privacy, the Complainant was told he had to follow the proper chain of command in the workplace and address his concerns to his manager. He was threatened with further disciplinary action if he persisted in seeking an explanation from the CEO.

"No person should ever feel constrained, for any reason, from standing up for his or her right to insist on the absolute privacy of his or her personal health records. I cannot think of a situation in which an employee should be disciplined for making such an inquiry or filing such a complaint."

Two internal investigations were eventually done to investigate the Applicant's allegations - one informal and one more formal. Both of these investigations found that there had been no breach of the Complainant's privacy, though the Complainant was at no time interviewed by either of the investigators and no details about the findings were provided to him. To make matters worse, a copy of the more formal report was provided not only to the Complainant, but also to his Manager and a number of other

individuals within the organization as well, presumably as part of the Complainant's employee file.

The public body denied that any information from the employee's medical record had been used at the disciplinary meeting. Rather, the information provided was merely gathered by means of observation, and conclusions reached based on those observations and a general knowledge of other facts.

"There was no reason whatsoever for the investigator's report, which was prepared as a result of a patient's concern about the security of his health file, to be provided to anyone other than the CEO and the patient with the concerns."

While satisfied that the manager had not at any time looked directly into the Complainant's personal health file, the IPC noted that if information about the Complainant's medical issues was available to the manager only as a result of her position in the public body, it's use in another proceeding, including disciplinary proceedings, would be an unauthorized use of the information without his consent. In this case, however, there was evidence that the Complainant himself had provided his manager with a letter from the doctor about his condition and the rest of the information she had simply assumed from the circumstances. In the end, there was not enough to conclude that there had been a breach of the Complainant's personal health information.

In the discussion of the circumstances, the IPC commented on the wide circulation of the internal investigation report and particularly that the privacy breach concern was seen as something that needed to be recorded on the employee's record. The IPC strongly condemned the connection of the privately filed com-

plaint to the individual's employment situation. The Complainant had asked the CEO to address what he considered to be a breach of his privacy not as an employee, but as a private citizen. There was no reason for the report to be placed on his personnel file or even to share the fact that a complaint had been made with anyone else in the workplace. It was not an employment matter at all.

The IPC recommended that BDHSSA take steps to review their policies and procedures as they relate to the privacy of the health records of employees and how and when those records can be used. She further recommended clear policies be created that will allow a patient who also happens to be an employee to make a privacy complaint concerning the use or disclosure of their own personal health information without being threatened with consequences within their employment.

The recommendations were accepted and BDHSSA committed to initiate steps to review their current policies with respect to the health records of employees and how and when they can be used. They further committed to develop policies clearly stating employee's rights to file a complaint regarding a breach of their privacy without fear of being penalized or disciplined.

REVIEW RECOMMENDATION 12-106

A complaint was made by a patient of the BDHSSA that his personal health information had been compromised. The Complainant in this case was, as in the previous case, also an employee of the BDHSSA. Here, the Complainant had received medical attention from the emergency department at the Inuvik hospital. He requested that access to his personal "paper" medical record be restricted because he did not want others in the workplace to be privy to his medical issues. While his paper records were secured immediately, the Complainant belatedly considered the possibility that his electronic records might not be similarly secured. He requested an audit of the electronic record and that audit revealed that there had been 12 instances in which his electronic record had been viewed by a combination of medical and clinical clerical staff outside of the time period in which he was receiving medical attention.

"Individuals have the right to know who has accessed their records and for what purpose. If the health authority cannot do that, there is a flaw in the system."

The electronic records system in place in the Inuvik hospital records every time a record is accessed and can identify the "user" who accessed the file. The system is also supposed to require users to identify the reasons for the access. Access to the system was controlled by the requirement to provide user name. Every employee was given a unique user name, but in some instances

access to the system could also be gained by means of generic user names, such as "emerg" or "clinic".

A review of the audit report was able to confirm that, for the majority of the 12 times that the Complainant's information had been accessed other than for direct treatment, the access was for legitimate reasons - for billing, to register the ER case, to send information to the WSCC, to register a lab event, or some other clearly legitimate purpose associated with the patient's health or health care. However, there were several audit hits which showed that the specific user was not identified (i.e. the "user" was 'emerg' or 'clinic') and several for which no reason has been recorded for the access.

"In my opinion, the onus lies on the health authorities to provide evidence that all access to an individual's personal health records is proper and for a legitimate reason under the *Act*. To suggest….that there is some need for the complainant to provide a motive which would point to an inappropriate use or disclosure of his personal health information is, quite simply, the wrong approach."

BDHSSA argued that the audit does not, in and of itself, establish any improper use or disclosure of personal health information. They also argued that even where the audit was not able to verify either the individual user or the reason for the viewing, there was no evidence to suggest that the information on the file had been improperly used or disclosed.

The IPC identified a number of concerns, particularly with respect to those instances which access was by a generic user rather than by an identifiable individual user and where there was no note indicated showing the reason for the access. The IPC was also concerned that the BDHSSA wanted to put the onus on the Complainant to establish that the access to his records was im-

proper when the Act clearly puts the onus on public bodies to ensure that the records are secure. The IPC also commented that any unauthorized access to or viewing of a patient file, whether or not the information is used or disclosed further, is a breach of the patient's privacy, particularly in a small community where everyone is connected to everyone else in some way or another. Unless there is a medical or associated administrative reason for viewing the record, the viewing of the record is unauthorized and inappropriate. The IPC made 6 recommendations:

"It is important for health authorities to understand that *any* unauthorized access to or viewing of a patient's medical record, whether or not the information is used or disclosed any further, is a breach of the patient's privacy…. Unless there is a medical or associated administrative reason for viewing the record….the viewing of the record itself is inappropriate and a breach of the patient's privacy."

1. that BDHSSA conduct a thorough Privacy Impact Assessment on the electronic record system at the Inuvik hospital and that steps be taken to improve the security and controls within the system based on the results of the PIA;
2. that steps be taken to immediately remove all generic user names and passwords from the system;
3. that steps be taken to ensure that every access to the system includes a reason for the access;
4. that BDHSSA prepare and implement a privacy orientation session as mandatory for all employees;
5. that there be constant, ongoing messaging provided to em ployees to reinforce the importance of privacy with respect to health records;
6. that immediate steps be taken to institute a system of regular random audits of the system.

The public body disagreed with the IPC's conclusion that the onus was on the public body to establish that there had been no unauthorized access to the Complainant's medical record and that

unauthorized access constituted a breach of the privacy provisions of the Act. That said, they accepted the recommendations made, in full.

REVIEW RECOMMENDATION 12-107

"That said, the Government of the Northwest Territories has a legislated mandate to respond to Access to Information requests within 30 days or, in certain narrow circumstances, within a 'reasonable' extended period of time."

A lawyer acting on behalf of claimants under the Residential School settlement asked me to review the length of time it was taking to get information necessary to make and support these claims from the Department of Education. She provided examples of a number of requests for access to information which had taken a year or more to respond to, rather than the 30 days provided for in the Access to Information and Protection of Privacy Act.

The department acknowledged that they had been receiving an increasing number of requests for information as a result of the residential schools question. Between 2005 and July of 2011, they had received a total of 1265 requests and had been able to respond fully to only 894 of those, leaving 371 outstanding requests, some of which had been made as far back as 2005. While efforts to streamline processes and hire additional staff and thereby shorten response times had been undertaken, the department was still significantly behind in responding.

The IPC noted that there was a 30 day response time contemplated by the Act. She referred as well to the provisions in the Act which allow for an extension of time in certain circumstances, pointing out that the department did not seem to be following the steps required in the Act for such extensions. She found, however, that the department had been working hard and in good faith to respond to all of the requests they received.

The IPC recommended that the Department of Education, Culture and Employment and NWT Archives

a) hire whatever staff was necessary to clear up the existing backlog within 90 days of the date of her report;

b) ensure that there are sufficient full time positions within the Department and/or NWT Archives on an ongoing basis whose job description is limited to responding to ATIPP requests;

c) take steps to ensure that, when extending the time for responding to requests for information, the appropriate procedures are followed;

d) that the department report to the office of the In formation and Privacy Commissioner on a bi-monthly basis until such time as the backlog was cleared.

"There must be sufficient manpower dedicated to getting these requests dealt with on a timely basis to ensure that any delays beyond 30 days are minimal."

The Recommendations were accepted. In the months since this report was issued, the Department has been able to reduce its backlog significantly, and there are now considerably fewer very old files left incomplete.

REVIEW RECOMMENDATION 12-108

A consultant requested a copy of the Barren Ground Caribou Harvesting Interim Agreement between the Department of Environment and Natural Resources (ENR) and the Yellowknives Dene First Nation (YDFN), an intergovernmental agreement between the Government of the NWT and the YDFN concerning the management of caribou herds. There was some controversy surrounding the agreement and a good deal of public interest in it.

"The *Access to Information and Protection of Privacy Act* governs the right of the public to access to information and informal assurances of confidentiality take a back seat to these rights."

ENR refused to disclose any part of the agreement on the basis that its disclosure could reasonably be expected to impair relations between the Government of the Northwest Territories and the YDFN.

On being consulted, YDFN made it absolutely clear that they objected strenuously to the disclosure of any part of the Agreement, even those parts that merely outlined the background issues. The Department also pointed out that they had provided YDFN verbal assurances that the agreement would be kept confidential unless YDFN agreed to the disclosure of all or part of it. The Applicant, on the other hand, pointed out that the agreement concerned an issue of significant public interest and argued that, while the YDFN did not want the agreement to be disclosed, there really was no real evidence that there would be negative consequences of any kind if the details were disclosed. He argued that wildlife management and conservation were matters of public gov-

ernment which should be open to public scrutiny and the fact that it might also be politically sensitive or controversial was not a justification for non-disclosure.

The IPC pointed out that the purpose of the *Access to Information and Protection of Privacy Act* is to facilitate democracy and that any exception to the right of access must be narrowly interpreted. She also observed that YDFN is a First Nations governing body, and therefore meets the definition of "another government" pursuant to Section 16 of the Act . This section provides public bodies with the discretion to refuse access to certain records where the disclosure could be reasonably expected to impair relations between the GNWT and "another government".

"As a democratic government within Canada, at some point YKDFN will likely have to come to terms with requests for access to its records. For now, however, YKDFN is not subject to the rules for access to information contained in the *Access to Information and Protection of Privacy Act*. "

During the review process, the IPC sought input directly from YDFN. The YDFN expressed adamant opposition to the disclosure of the report. They were concerned that if the agreement were to be disclosed, it would create controversy, draw criticism or invite inquiries.

The IPC concluded that while such concerns would not relieve a public body of the obligation to disclose, YDFN is not a public body under the Act and is not, therefore, subject to the same rules. Because YDFN had expressed it's objections so strenuously, the IPC found that there was a reasonable expectation that the disclosure of the record would impair relations between the two governments and the discretion to refuse access, therefore, arose.

The IPC recommended:

a) that ENR fully analyze their position with respect to the disclosure of the Agreement, bearing in mind the overriding purposes of the Act is that disclosure is the rule and exceptions should be interpreted narrowly;

b) that ENR carefully consider, in particular, the possibility of disclosing those portions of the Agreement which are already within public knowledge including those portions of the Agreement which state historical facts and background only;

"What is in issue is whether there is a reasonable likelihood that the relations between the two governments would be harmed or impaired by the disclosure and I am satisfied, based on the submissions of the YKDFN, that the relationship between the two governments would be negatively impacted."

The department, after discussions with the YDFN Chiefs, "determined that the relationship between the two governments (GNWT/Akaicho) would be harmed, jeopardizing future negotiations including land claims and caribou management cooperative agreements." They concluded that the loss of trust between the two parties would outweigh the public policy benefit of accountability and transparency in this case. They therefore exercised their discretion and refused to disclose the agreement.

REVIEW RECOMMENDATION 12-109

The Complainant, an employee of the Government of the Northwest Territories with a number of physical and psychological challenges, was of the opinion that Yellowknife

Social Services (YHSS) and his personal physician had improperly disclosed his personal health information. The Complainant's situation was such that he required workplace accommodations and it was agreed that he should have a psychiatric assessment done to facilitate discussions about what accommodations would be best to meet his needs. The Complainant says that he was assured that the information from the psychiatrist would not be shared with his employer. Despite this, the Complainant alleged that the physician sent the employer a letter about the assessment and that a full copy of the psychiatric report had been attached.

The physician, on the other hand, said that he reviewed the psychiatric report with the Complainant in person and that they both agreed that the report should be provided to the employer. The physician acknowledged that he had prepared a letter for the employer and that he had attached a copy of the psychiatric report to that letter. He denied, however, that anyone in his office ever provided the letter to the employer. Even if the letter was delivered to the employer by YHSS, the health authority argued that they had the Complainant's written consent to share the information. The public body had no record of the letter going out its door, but a staff member recalled that the Complainant had attended the office, read both the letter and the consultation report and had then signed a consent that both be disclosed to the employer. The public body suggested that it was

likely the Complainant who had, in fact, delivered the letter the employer.

Regardless of how it got there, all concede that the letter with its attachment was delivered to the Complainant's employer. Before it was opened, however, the Complainant recovered it, unopened and unread.

"While the oath of confidentiality is meant to prevent the discussion of personal information outside of the workplace, this does not address unauthorized or inappropriate access to personal health records. These are two different… issues."

The IPC found that, because the letter was recovered from the employer before it had been reviewed, there was no actual disclosure. She was concerned, however, that the public body in this case could not confirm how or when the letter had left their office. She commented, as well, on the fact that the consent form signed by the Complainant was lacking. The name and the address of the intended recipient was blank. She pointed out that it is the public body's responsibility to ensure that they have the appropriate consent to the disclosure of information and, in the case of sensitive medical records, a verbal consent, or an apparent consent is not enough. Thirdly, she expressed concern that the physician described the information in the consultation report as "matter of fact" when it contained a significant amount of historical medical information which was very private in nature. Further, it appeared that the physician did not appear to appreciate the delicacy of the situation or the importance of recording discussions in which consent is verbally discussed, noting that there had been no notes on the Complainant's file concerning his discussion with the physician.

The IPC made several recommendations, including:

a) that a system be developed for dealing with consents for the release of health information with specific procedures to be followed, including a checklist for support staff to ensure that every step in the process is followed, that all necessary information is filled out on consent forms, and that there is space available for the patient to make any notes or give any specific instructions they might have;

b) that when patients request the disclosure of personal health information to third parties, such as employers and/or insurance companies, physicians be encouraged to make notes on the patient's file to confirm when a discussion takes place about the disclosure and any instructions received from the patient.

The recommendations were accepted.

"...it is the public body who must account for the collection, use and disclosure of personal information and it is therefore their responsibility to ensure that these [consent] forms are fully and correctly completed. It is not sufficient for the public body to rely on a verbal direction when dealing with personal health information."

REVIEW RECOMMENDATION 12-110

The Complainant had a history of mental health issues, for which he was on medication. His treatment was ongoing. At one point, the Complainant attended an appointment with his primary care physician at which time he says his physician told him that members of his family had come to see him to discuss the Complainant's behaviour and to express their concern about the Complainant's mental health. This had been confirmed in

discussions with those same family members who admitted to the Complainant that they had discussed his behaviour with the physician. There were no notes on the Complainant's medical file which would confirm that the physician had discussed matters with the Complainant's family members.

YHSS confirmed that the physician had, in fact, met with members of the Complainant's family but denied that he had discussed the Complainant with them. Rather, they say that the physician met with the family members to provide them with medical care of their own.

"When physicians are faced with someone offering gratuitous personal health information about a third party, it is incumbent upon the physician to stop the conversation as quickly as possible.

The IPC was satisfied, based on the information provided by all parties to the review, that there had most likely been some discussions between the physician and the Complainant's family members about the Complainant. There was, however, no evidence to suggest that the doctor initiated those conversations, or that he engaged in them other than to suggest that the Complainant needed to seek medical attention. The IPC observed that while a physician cannot control what comes out of the mouth of a patient, he can control how he responds. There was, in this case, simply no evidence that the physician had done anything other than acknowledge the concerns of the family members and suggest that the Complainant seek help. There was, in this, no breach of privacy. As a result, no recommendations were made. The public body did not provide any response to the comments made by the IPC.

REVIEW RECOMMENDATION 12-111

An Applicant sought access to records from the Department of Industry, Tourism and Investment in relation to duplicate or replacement certificates issued by the department under the GNWT's Certified Canadian Diamonds program. After conducting third party consultations, the public body disclosed aggregate numbers of replacement certificates issued and the names of some of the businesses which had requested them. They refused to disclose the names of certain other businesses on the basis that the disclosure could be reasonably expected to result in undue financial loss or gain or to prejudice the competitive position of the third party. They also refused to name individuals (as opposed to companies) who had received duplicate certificates on the basis that this would constitute an unreasonable invasion of the individual's privacy. Finally, they refused to disclose the actual number of duplicate certificates issued to each company or the criteria under which the duplicate certificates had been issued.

The IPC acknowledged that the disclosure of the names of the two individuals who had received duplicate certificates should not be disclosed, as to do so would be an unreasonable invasion of their personal privacy. However, if the names of the individuals who received the duplicate certificates were withheld, there was

no reason not to disclose background information about the reasons the certificates were issued.

The IPC did not agree with the department's refusal to disclose the names of two companies who did not respond to the third party consultation done by the department. The fact that the companies were engaged in the buying, selling or trading of diamonds is not information that is protected under the Act. The IPC could also find no any evidence that the disclosure of the specific information requested by the Applicant would harm the business interests of any of the companies involved.

"If the names of the individuals requesting the certificates are withheld, there is no personal information left, and no reason not to provide the Applicant with the specifics requested."

The IPC recommended that, provided that the Applicant was satisfied to receive "information" as opposed to "records", the public body disclose the names of all the companies who had requested and/or received duplicate certificates, the number of duplicate certificates issue to each company, the criteria under which the certificates had been issued, and the number of duplicate certificates that had been issued to individuals, as well as the criteria used, but not the names of the individuals involved.

The review recommendations were accepted.

REVIEW RECOMMENDATION 12-112

The Complainant's employer asked him to obtain a letter of prognosis from his physician. To this end, he signed his consent on a form entitled "Employee Request for Medical Prognosis" and provided that, along with a copy of a letter from his employer outlining the information they were seeking, to his physician. The letter was addressed to the Complainant. It had also been copied to various people within the Human Resources department of the employer. The consent on the Employee Request for Medical Prognosis form was worded as follows:

> I hereby authorize the Health Practitioner to release the information to myself and/or the Government of the Northwest Territories

"In this case, the consent provided by the Complainant is equivocal. It provides a consent to the release of 'prognosis information' to 'myself and/or the Government of the Northwest Territories'.

The Complainant understood that the physician would complete the form and give it to him to pass on to his employer. Instead, the physician provided the employer with the completed form which contained his consent, along with a detailed letter outlining a number of other medical details. In addition, the physician chose to copy both the form and the letter to all of the Human Resources people who had been copied on the letter which the Complainant had received from his employer.

It was the public body's position that the Complainant had provided his consent to the disclosure of this personal information to

"the Government of the Northwest Territories" and that was sufficient to allow the disclosure to all of the people who had received a copy of the report.

The IPC observed that the consent form relied on by the public body was equivocal and open to a very wide interpretation. The "and/or" made the consent unclear unless one of the two words was highlighted in some way. Furthermore, the "Government of the Northwest Territories" is a very large entity. Nor did the consent appear to allow for the disclosure of information that went beyond the four corners of the form the consent was attached to.

"The [doctor's report] should have been directed only to the Complainant's supervisor. ….This is NOT just semantics or a technicality. This is about the law which restricts public bodies and employees of public bodies from using or disclosing the personal information of individuals except in accordance with the Act. "

The IPC concluded that there had been a breach of the Applicant's privacy, in particular as a result of the wide distribution of the form completed by the physician and the letter which accompanied it.

The IPC recommended:

1. that the "consent" part of the "GNWT Employee Request for Medical Prognosis" be revised so as to:
    a) require the person consenting to identify specifically who the information is to be disclosed to;
    b) remove the "and/or" from the consent form;
    c) specify that the consent relates only to the information outlined in the attached form, unless there is a specific authorization from the patient to the physician to add any additional information that might be necessary

2. that all health care workers, particularly physicians, be given more training or at least more information about when and in what circumstances they can disclose the personal health information of patients to third parties

3. that practices and procedures be developed with respect to what is required of health care workers when obtaining consent to the disclosure of personal health information so that both the process and the message is consistent.

The public body did not accept the IPC's analysis of the issue. They were of the opinion that the form of consent signed by the Complainant was sufficient to authorize the physician to respond directly to the employer and that he did so properly. They were prepared to accept that the consent was equivocal, but indicated that they could not conclude that the physician acted unreasonably in completing the form while providing an additional separate letter. They did not accept that in providing the employer with both the completed form and a letter with additional information was a breach of the patient's privacy. Nor did they accept that providing a copy of the physician's report to all of those who were copied resulted in any breach of the patient's privacy because "the result was ultimately consistent with the purpose for which the information was collected and compiled".

The public body ultimately agreed to forward the IPC's recommendation with respect to the GNWT's medical prognosis form to the Department of Human Resources. They further agreed to pass on the recommendations with respect to the practices and

procedures surrounding the obtaining of consent to the Department of Health and Social Services. They did not agree to review their own practices in this regard.

REVIEW RECOMMENDATION 12-113

The Applicant sought information about polar bear harvesting in the Northwest Territories. Some information was provided but the public body refused to disclose the latitudinal and longitudinal information about bear kills on the basis that it would identify locations where these animals are found. The department contended that the polar bear has been identified as a species at risk under federal legislation and they were of the opinion that the disclosure of this particular information could result in additional risk to, or could be detrimental to the survival of the species. The Applicant provided a number of scientific facts about polar bear populations which suggested that the disclosure of polar bear kill sites would be unlikely to provide hunters with any significant advantage or create a greater possibility that polar bears could be located. The department provided equally compelling scientific information which suggested that exactly the opposite was true.

The IPC found that Section 19 of the *Access to Information and Protection of Privacy Act* gives public bodies a discretion to refuse

to disclose information where the disclosure could reasonably be expected to result in damage to or interfere with the conservation of a rare or endangered, threatened or vulnerable life form. Compelling arguments were made on both sides of that argument but the IPC was satisfied that the public body had raised legitimate and reasonable concerns about the disclosure of the information requested and had properly refused to provide latitudinal and longitudinal specifics of kill sites. No further recommendations were made.

The Minister acknowledged and accepted the findings.

"If the supervisor in this case is able to complete his/her supervisory functions without the names and addresses of the clients **seen by the counselors in a call out situation, that information should not be either required or provided."**

REVIEW RECOMMENDATION 12-114

The Complainant was an employee of a regional health authority, working in a small community as a counsellor. His concerns arose from the requirement imposed on him to provide detailed patient information to headquarters when called on to deal with incidents after regular working hours. He objected to having to provide the names and addresses of his clients on the required forms because that kind of disclosure was contrary to his professional obligation to protect the confidentiality of his clients. When he raised this as an issue, he was advised that unless he provided all of the information requested in the "call out" forms, he would not be paid for his overtime.

The call out forms required the counsellor to provide the name and phone number of the person who requested the call out, the name of the employee, the date and time of the call, as well as the name, address and telephone number of the client and the reason for the call out, a summary of what the issue was, what the employee did, what the current status of the matter was and what follow up was required.

"I am not convinced that, except in very rare circumstances, will it be necessary for the supervisor to know the name and address of the client in order to provide proper supervision of the worker. If, for some reason, the name and address of the client becomes necessary to supervise the employee, the information can be retrieved from the client file on an individual basis as needed."

The health authority argued that there were a number of reasons for the requirement to complete the call out form. Firstly, there was a legal requirement to chart health incidents and place it on the client's chart as part of his/her permanent record. There was also a risk management component to the form in that it would allow supervisors to review and monitor the actions taken by staff and ensure continuity of care and necessary follow up in a timely and appropriate manner. The form was also used for program evaluation to ensure appropriate staffing levels and service provision models appropriate for each community. Finally the form was used as a tool to ensure accurate compensation for on call services provided by the employee. The Supervisor, in this case, is in a different community and rarely, if ever, had direct contact with the client.

The health authority argued that all employees of the authority have sworn an oath of confidentiality and are aware of the importance of maintaining client confidentiality. They also argued that the supervisor was within the client's "circle of care" as they are employed within the same program area as the counsellor.

The IPC was not persuaded that it was necessary for information which would have the result of identifying clients and their personal health information to be provided to headquarters. She pointed out that one of the 10 privacy principles was to gather, use or disclose the least amount of information necessary for any particular purpose. She found that while it was appropriate to be collecting all of the information on the call out form for the purposes of legal charting, there was no real reason for all of that information to be provided to headquarters for the purposes of administration. While continuity of care was an important goal, if headquarters really needed this information to achieve this goal, they would be asking the community employees to provide this kind of information for all patients, not just those who received services after hours.

"Privacy is much more than confidentiality. While the oath of confidentiality is an excellent and necessary starting point for protection against the inappropriate use and/or disclosure of personal health information, it is far from perfect in terms of end result. Human nature being what it is, it would be folly to rely only on that oath to prevent inappropriate uses or disclosures of personal information ."

The IPC recommended that:

a) the health authority immediately discontinue the requirement that counsellors provide client names and and addresses for the purposes of reporting on after hours call outs and that they redraft their reporting forms such as to collect the minimum amount of information necessary for the supervisor to complete her job responsibilities; and

b) the health authority discontinue the use of the term "circle of care" to justify the use and disclosure of personal health information at least until some reasonable definition of that term has been established, based on what a patient would understand to be the medical "circle of care" in any particular situation.

The first of these recommendations was accepted. The health authority, however, refused to accept the recommendation with respect to the term "circle of care".

REVIEW RECOMMENDATION 13-115

The Complainant was the recipient of a faxed copy of some sensitive personal health information of a third party stranger. The fax had been sent by the Yellowknife Primary Care Clinic (YPCC) via a "scan to email" function from a photocopy machine. Within minutes, the recipient received a second fax from YPCC, asking the recipient to destroy the last email sent.

In responding to the complaint, YPCC explained that the Complainant was a patient at the clinic and that the only way they had to communicate with him was by email. The patient did not own a land line or a cell phone, but he did have an internet connection and he had asked the clinic to send an email to his personal email address when they needed to contact him. This was not a way they normally communicated with patients, but was done as an accommodation for this particular patient. The error which resulted in the misdirected fax was, they said ,as a result of human/technical error, but no further explanation was provided. As a result of this complaint, the YPCC discontinued their practice of communicating with the Complainant via "scan to email".

The IPC acknowledged that whenever human beings are involved in anything, there is the possibility that an error might be made and she appreciated the fact that in this case the YPCC recognized the mistake immediately and did what they could to recall the

misdirected information. That said, she expressed concerns that, in this day and age, no policies had yet been developed for the use of "non-traditional" means of communicating with patients. Where the patient has consented to the use of email for communicating with him/her, that should be a viable option. But there have to be policies and procedures in place for that to happen.

"We learn from our mistakes and the public body should be able to identify exactly how the mistake was made, and what needs to be done to prevent it from happening again. Simply shutting down that avenue of communication is not necessarily the answer, particularly, as noted above, where the public is moving more and more toward the use of electronic means of communication."

The IPC was also concerned that YPCC could not provide any real specifics about what went wrong and how the third party's information ended up being sent to the Complainant other than that it was "human error". She noted that if you cannot pinpoint exactly what happened, you cannot effectively address the error so that it doesn't happen again.

The IPC recommended that YHSSA take immediate steps to develop and implement policies for communicating with patients via non-conventional means, including email, fax to email, text messaging and other electronic means, keeping in mind the additional risks to privacy that might need to be addressed.

The recommendations as to change were accepted, but the proposed time line for such changes to be in place was not. No time frame was provided.

REVIEW RECOMMENDATION 13-116

The Complainant was convinced that his adoption records had been improperly used or disclosed. He had been adopted more than 40 years previously from a small community in what is now Nunavut. He alleged that some time between 1997 and 2000, his adoptive sister contacted him and told him that she had two telephone numbers for him. One was for an adoption worker in Yellowknife and the other was for his natural mother, who had been trying to find and reconnect with him. He says that he had never been interested in knowing his biological mother, but he took his mother's phone number and eventually decided to use it. His experience in reconnecting was not positive.

In 2012, the Complainant contacted the Department of Health and Social Services to obtain a copy of his adoption file so that he could find out how and why his adoptive sister had been given access to his personal information. He was told that he needed to fill out a form, in which he was asked to provide a significant amount of other personal information. The form is used by the department to help them locate adoptive relatives on request. The Complainant refused to fill out the form because he was not looking to reconnect with family but, rather, was trying to find out how information from his adoption file had ended up in the hands of his adoptive sister.

The department indicated that the Complainant's natural mother had contacted them looking to reconnect with her son. The *Adoption Act* gives the Director of Adoptions the authority to make discrete inquiries when an adopted child or a biological family member seeks to reconnect with family. In this case, in order to find the Complainant, the director contacted the Complainant's sister and asked her to have him contact the department. There is no evidence on the file, they say, that suggests that the sister was provided with any information about the biological mother or about the Complainant.

The IPC reviewed the Complainant's file and confirmed that there was nothing on the file to suggest that the sister had been provided with any information about the Complainant or his mother other than that the department was attempting to find him and that the Complainant's mother was interested in contacting him. There was, however, very little detail in the file that would allow a reader to determine exactly what happened. There is evidence that the Complainant contacted the director and was provided with his mother's contact information. It is also clear from the file that the Complainant eventually decided to contact his birth mother.

The IPC also commented on the way in which the Director of Adoptions addressed the Complainant's inquiry. They had treated it as a request for access to his adoption records under the *Adoption Act*, rather than as request under the *Access to Information and Protection of Privacy Act*. What the Complainant in this case was seeking was not information that would connect him to his biological family, but information about how his personal information had been used or disclosed.

The IPC recommended that, in relation to the disclosure of information from the Adoption Registry:

a) all conversations with birth families seeking reunification be recorded and clear notes be made of who made the contact, what the nature of the conversation was and what next steps were agreed upon;

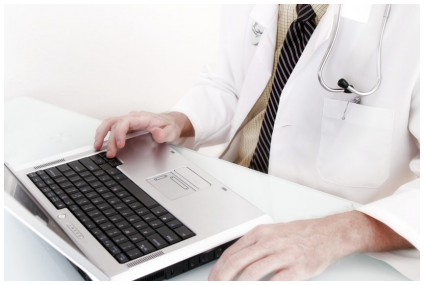
b) before information about birth family is provided to any other member of the family, there be a written consent to the disclosure obtained and kept on file;

c) when looking for birth families, case workers disclose as little information as is possible to third parties about the reasons they are looking for the individual or individuals;

With respect to the Complainant's request to see all records which relate to how he and his birth mother came to be reunited, the IPC recommended that the Complainant's request be treated as and Access to Information Request and that he be provided with all the relevant records relating to the matter.

The recommendations were accepted.

LOOKING AHEAD

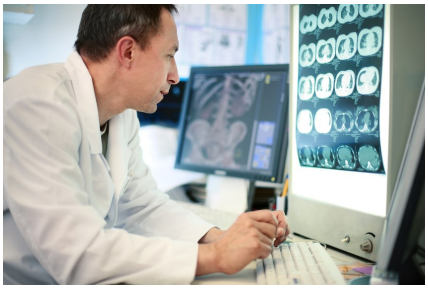


The fact that there have been so many complaints coming across my desk which focus on concerns about the privacy of personal health information points to the need for health information legislation. I am pleased, therefore, to know that the Government of the Northwest Territories is working on legislation to address, specifically, privacy issues in the health sector and that the tabling of that legislation is imminent. That said, this legislation will require a significant investment in education — the education of those working in the health sector as well as the education of the public. Other Canadian jurisdictions which have implemented similar legislation have all found that they have needed time and resources in the run up to the coming into force of health privacy legislation so as to make sure that everyone has the information they need to properly understand the legislation and prepare for it. There will be a need to develop and implement new policies and procedures on the part of health information custodians. There will have to be considerable work done to ensure that the public has a good working understanding of how their personal health information will be collected, used and disclosed under the

Act. New legislation is only part of the equation. The necessary resources have to be put into the oversight function provided by the Office of the Information and Privacy Commissioner. This legislation will inevitably increase the work load of the Office and I anticipate that sooner, rather than later, this office will need to expand its numbers. I have been saying, for several years now, that for the Information and Privacy Commissioner to be able to do a fully effective job, it is increasingly necessary for me to spend more and more time doing the job. I anticipate that, with the passage of the Health Information Act, the work load will be increasing exponentially and it will be time to consider hiring a full time employee to assist with investigations, mediation and other dispute resolution functions.

Once again, I would encourage the Government of the Northwest Territories to find ways to include municipalities under the Act or under their own legislation. This is a recommendation I have been making for many years. The feedback I have received points to the additional cost that would be incurred by municipalities to comply with the access provisions of the Act. In my opinion, the cost associated is a necessary cost of transparency, accountability and, ultimately, democracy. That said, if the issue is the cost of complying with the access provisions of the Act, a short term alternative, which does not have the same cost implications, would be to make municipalities subject to the Part II of the Act — the provisions which relate to the collection, use and disclosure of personal information.

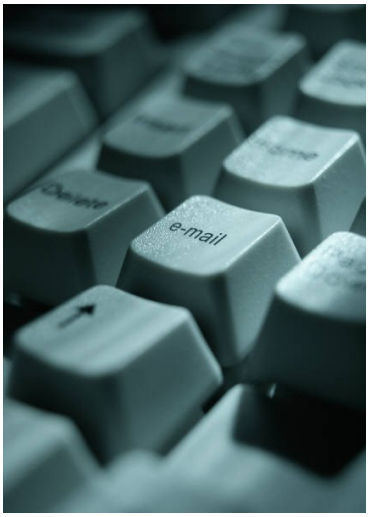
In light of the matters discussed in Review Recommendation 12-108, it seems to me that it may also be time to start the discussion about ensuring that First Nations governments in the Northwest Territories are also required to provide access to information in accordance with the principals of the *Access to Information and Protection of Privacy Act* and the Ten Principals of Protection of Privacy. I fully realize that this is not something that the Government of the Northwest Territories has control over, but I would encourage all levels of government to begin the discussion.



Finally, as introduced in the Information and Privacy Commissioner's Message, it is time for a review of the Act to ensure that it can effectively address changes in the government practices, (such as public/private partnerships, outsourcing or shared services models), changes in technology, and changes in the expectations of Canadians in terms of accountability of government agencies. Recent activist whistle blowers, like Julian Assange and Edward Snowdon, indicate a trend toward a public demand for more transparency and accountability in the work that governments do. Information is one of the most important natural resources there is in today's world. It is a valuable resource. It is a public resource. Access and privacy legislation needs to reflect the increasing value of this resource. At their Annual Meeting in 2012, the Information and Privacy Commissioners of Canada acknowledged that most access and privacy legislation in the country today has remained relatively unchanged since the 1980s and called upon Federal, Provincial and Territorial governments to modernize and strengthen these laws. I, in turn, call of the Government of the

Northwest Territories to do a comprehensive review of the Act with a view to introducing amendments to the Act which will, among other things:

- address the use of current day technologies;
- create a legislated duty requiring all public entities to properly document matters related to deliberations, actions and decisions;
- to provide for strict and enforceable time lines for response to access requests;
- to establish minimum standards for proactive disclosure;
- to establish legislative requirements for notifying affected individuals when their personal information has been lost, stolen or improperly accessed, used or disclosed; and
- to establish a requirement that, for any new legislation, service, program, or policy, public entities consider a plan for privacy implications at the outset, by requiring privacy impact assessments and instituting "Privacy by Design".



APPENDIX A

MODERNIZING ACCESS AND PRIVACY LAWS FOR THE 21ST CENTURY

CONTEXT

Canadians have come to expect greater accountability and transparency on the part of both governments and private-sector organizations with respect to how they gather, create, share, disclose and manage information, including personal information.

There have been many changes in technology, changes to government practices (such as public/private partnerships, outsourcing or shared services models), and Canadians' expectations over the years. Recent revelations about government surveillance programs have heightened Canadians' concerns about the erosion of their privacy rights and have prompted calls for increased transparency and greater oversight of national security initiatives.

Most Canadian access and privacy laws have not been fundamentally changed to keep up with these changes and to improve protections and rights since their passage, some more than 20 years ago. Only a few Canadian laws have recently been passed or updated to address modern challenges and to ensure continued protection of individuals' rights to access and privacy.

At the same time, other laws have been amended or passed that have had the result of undermining or eroding access and privacy rights – the very rights access and privacy laws were intended to protect and guarantee.

Elsewhere in the world, privacy and access laws are being strengthened to meet the realities of the 21st Century – more powerful information and communication technologies, the challenge of managing electronic information and the social and political demands of engaged citizens.
Canada's laws need to do the same.

WHEREAS

Information is one of Canada's most important national resources.

Robust protection of privacy and access to information are defining values for Canadians and underpin our democratic rights and freedoms.

Canadians need to be able to hold public institutions and private organizations to account for their privacy practices, their access decisions and their information management.

Canada must re-establish its position as a leader in both the access and privacy fields.

THEREFORE

1. Canada's Information and Privacy Commissioners and Ombudspersons call on our respective governments to recommit to the fundamental democratic values underpinning access and personal privacy legislation by:

    - Consulting with the public, civil society and Information and Privacy Commissioners and Ombudspersons on how best to modernize access and privacy legislation in light of modern information technologies, evolving government practices and citizens' expectations.

    - Modernizing and strengthening these laws in keeping with more current and progressive legislation in parts of Canada and around the world, including some or all of the following:

In terms of access to information:

a) Providing strong monitoring and enforcement powers such as the ability to issue binding orders for disclosure, and penalties for non-compliance;
b) broadening and clarifying which public entities are covered by access laws;
c) Creating a legislated duty requiring all public entities to document matters related to deliberations, actions and decisions;
d) Legislating strict and enforceable timelines for public entities to respond to access requests in a timely fashion;
e) For exemptions where the expectation of harm is in issue, limiting which records are exempt from the general right of access by requiring public entities to prove there is a real and significant harm in their disclosure;
f) Requiring all records, including exempt records, be disclosed if it is clearly in the public interest to do so;
g) Establishing minimum standards for proactive disclosure, including identifying classes or categories of records that public entities must proactively make available to the public and, in keeping with the goals of Open Data, make them available in a usable format;
h) Requiring that any exemptions and exclusions to access that are to be included in laws other than access to information laws be demonstrably necessary and that government consult with Information and Privacy Commissioners and Ombudspersons; and
i) Establishing a requirement that for any new systems that are created, public entities create them with access in mind, thus making exporting data possible and easier.

In terms of privacy:

a) Providing strong monitoring and enforcement powers and penalties for noncompliance;
b) Broadening and clarifying which public entities are covered by privacy laws;

c) Establishing legislative requirements for notifying affected individuals when their personal information has been lost, stolen, destroyed, or improperly accessed, used or disclosed (mandatory breach notification);
d) Requiring public and private entities to improve the information they provide about their personal information policies and practices;
e) Legislating a "necessity test" requiring public and private entities to demonstrate the need for the personal information they collect;
f) Providing individuals with effective means to assert their privacy rights and to challenge entities' compliance with their legislated obligations;
g) Strengthening reporting requirements to the public with respect to the disclosure of personal information between private and public entities;
h) Legislating a requirement that public and private entities implement privacy management programs to ensure the protection of personal information; and
i) Establishing a requirement that for any new legislation, service, program or policy, public entities consider and plan for privacy implications at the outset (for example, privacy impact assessments, privacy by design).

2) Canada's Information and Privacy Commissioners and Ombudspersons commit to"

- Engaging and following up with government, Legislature and Parliament on the issues set out above;
- Continuing to study and make public how access and privacy laws impact all Canadians; and
- Making recommendations to government, Legislature and Parliament based on our areas of expertise.

List of signatories

Jennifer Stoddart, Privacy Commissioner of Canada

Suzanne Legault, Information Commissioner of Canada

Elizabeth Denham, Information and Privacy Commissioner for British Columbia

Jill Clayton, Information and Privacy Commissioner of Alberta

Mel Holley, Acting Ombudsman for Manitoba

Anne E. Bertrand, Access to Information and Privacy Commissioner of New Brunswick

Ed Ring, Information and Privacy Commissioner for Newfoundland and Labrador

Elaine Keenan Bengts, Information and Privacy Commissioner for the Northwest Territories and Information and Privacy Commissioner for Nunavut

Dulcie McCallum, Freedom of Information and Protection of Privacy Review Officer (Commissioner) for the Province of Nova Scotia

Ann Cavoukian, Information and Privacy Commissioner of Ontario

Maria C. MacDonald, Information and Privacy Commissioner of Prince Edward Island

Me Jean Chartier, President, Commission d'accès à l'information du Québec

R. Gary Dickson, Information and Privacy Commissioner of Saskatchewan

Diane McLeod-McKay, Ombudsman and Information and Privacy Commissioner of Yukon

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

5018 - 47th Street
P.O. Box 262
Yellowknife, NT
X1A 2N2

Le 31 octobre 2013

Assemblée législative des Territoires du Nord-Ouest
C. P. 1320
Yellowknife NT X1A 2L9

À l'attention de : Madame Colette Langois
Greffier intérimaire de l'Assemblée législative

Madame,

J'ai l'honneur de déposer mon rapport annuel à l'Assemblée législative des Territoires du Nord-Ouest pour la période du 1er avril 2012 au 31 mars 2013.
Veuillez agréer, Monsieur, mes salutations les plus distinguées.

Elaine Keenan Bengts
Commissaire à l'information et à la protection de la vie privée
Territoires du Nord-Ouest

/kb

In Yellowknife: 867-669-0976 ♦ Toll free: 888-521-7088 ♦ Fax: 867-920-2511 ♦ E-mail: AtippComm@theedge.ca

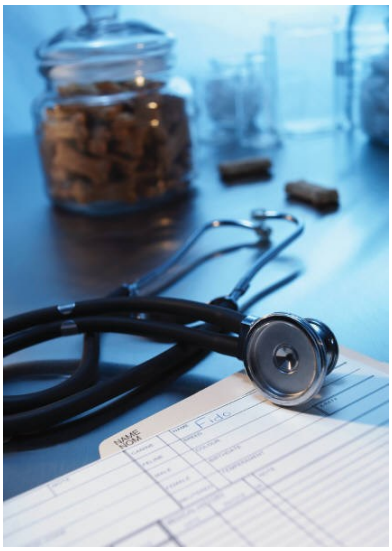
TABLE DES MATIÈRES

MESSAGE DE LA COMMISSAIRE

L'exercice 2012-2013 a très certainement été marqué par la question de la protection des renseignements médicaux. Seize nouveaux dossiers ont été ouverts cette année : sept d'entre eux touchaient de près ou de loin les renseignements médicaux. De plus, douze recommandations relatives à des demandes de révision ont été émises, et sept d'entre ells portaient sur la collecte, l'usage ou la divulgation de renseignements médicaux personnels. Les problèmes ont été soulevés notamment par des patients inquiets de la façon dont leurs renseignements médicaux personnels étaient partagés à l'intérieur même d'une administration des services de santé, ainsi que par des patients qui étaient également employés d'une administration des services de santé des Territoires du Nord-Ouest et qui se demandaient si leurs collègues et superviseurs avaient accès à leurs renseignements médicaux personnels. Enfin, il y a une fois de plus eu des cas où des renseignements médicaux personnels ont été envoyés par télécopieur au mauvais destinataire.

Ce qui est clair, c'est que le public se sent très interpellé par la question de la protection des renseignements médicaux. Dans un grand nombre de cas, il semble y avoir un manque de compréhension de la part du public à propos de la façon dont les

renseignements sont réellement partagés et utilisés au sein du système de santé. Qui plus est, il semblerait que les administrateurs de la santé aient de la difficulté à reconnaître que les renseignements médicaux relèvent de la vie privée et que le patient a droit à un certain contrôle sur ses propres rensegnements. C'est pourquoi il est d'autant plus important de nous assurer que le projet de loi sur les renseignements médicaux sera mis de l'avant pour être débattu et examiné le plus rapidement possible. De plus, lorsque le projet de loi sera déposé, il faudra s'assurer que la population prend part à son examen. Le public fait généralement confiance aux administrations des services de santé quand il est question de protéger leurs renseignements médicaux personnels, mais une fuite peut avoir de très graves conséquences pour la personne concernée. Le système de santé est très complexe, et le partage des renseignements est essentiel à son fonctionnement. Ceci est d'autant plus vrai dans le Nord, où les patients doivent souvent se déplacer ailleurs dans le territoire ou dans une autre province pour obtenir les traitements qu'il leur faut, en quel cas leurs renseignements doivent les suivre. Les gens doivent faire confiance au système qui est en train de se mettre en place. Ils doivent avoir la certitude que, sauf s'ils doivent être partagés, leurs renseignements médicaux personnels ne seront utilisés que ce pour quoi ils ont été amassés, et qu'ils peuvent contrôler qui y a accès. Je souhaite donc voir la nouvelle loi sur les renseignements médicaux personnels entrer en vigueur le plus rapidement possible. Lorsque ce sera chose faite, de nouvelles ressources



devront être allouées au Commissariat à l'information et à la protection de la vie privée afin de gérer les responsabilités accrues en matière de surveillance qui découleront de la nouvelle loi.

Bien que la protection des renseignements médicaux ait occupé une grande partie de mon emploi du temps cette année, il y a aussi eu d'autres enjeux. Depuis plusieurs années, je demande au gouvernement des Territoires du Nord-Ouest d'effectuer un examen approfondi de la *Loi sur l'accès à l'information et la protection de la vie privée* (la Loi). Fait intéressant, en août 2012, lors d'une rencontre réunissant mes collègues de partout au pays, les commissaires à l'information et à la protection de la vie privée du Canada ont passé à l'unanimité une résolution afin de sommer les gouvernements provinciaux, territoriaux et fédéral à réaffirmer leur engagement envers les valeurs démocratiques qui sont à la base des lois sur l'accès à l'information et la protection de la vie privée, en consultant le public, la société civile ainsi que les commissaires à l'information et à la protection de la vie privée. On voulait ainsi déterminer la meilleure façon de mettre à jour ces lois en tenant compte des nouvelles technologies de l'information ainsi que de l'évolution des pratiques gouvernementales et des attentes des citoyens. Les gouvernements doivent aussi mettre à jour et renforcer ces lois pour emboîter le pas aux lois plus modernes et progressives en vigueur ailleurs dans le monde. Une copie de cette résolution est présentée en annexe à la fin du present rapport annuel. Elizabeth Denham, la commissaire à

l'information et à la protection de la vie privée de la Colombie-Britannique, note ce qui suit dans son plus récent rapport annuel :

> Dans le secteur privé, les consommateurs ont encore un certain degré de liberté lorsque vient le temps de choisir où et avec qui ils désirent partager leurs renseignements personnels. Lorsqu'ils ont affaire au gouvernement, ils n'ont pas cette liberté. En effet, les citoyens n'ont d'autres choix que de partager leurs renseignements ersonnels pour se prévaloir de soins de santé ou de services, comme l'obtention d'un permis de conduire ou d'un passeport.
>
> Il est donc impératif que les organismes publics mettent en place de nouveaux systèmes de gestion de l'information afin d'offrir ces services tout en protégeant a vie privée. Ils devront être surveillés par un organisme indépendant pendant l'élaboration de ces programmes.

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

La Loi sur l'accès à l'information et la protection de la vie privée se fonde sur deux principes :

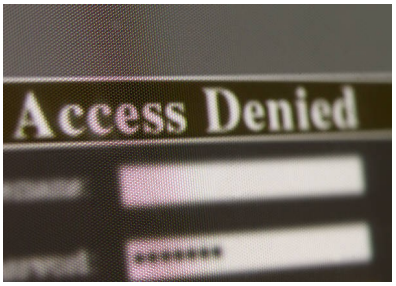
1. les documents publics doivent être accessibles au public;
2. les renseignements personnels doivent être protégés par les organismes publics.

La Loi définit les règles concernant l'accès aux documents publics; elle décrit aussi celles entourant la collecte, l'usage et la divulgation de renseignements personnels par les organismes publics des Territoires du Nord-Ouest (TNO).

La Loi s'applique à tous les organismes publics des TNO, incluant l'ensemble des ministères et des sociétés d'État ainsi que certains conseils et certaines commissions et agences.

La Cour suprême du Canada a déclaré que les lois comme la *Loi sur l'accès à l'information et la protection de la vie privée* sont des instruments spéciaux qui définissent certains des droits démocratiques fondamentaux que possèdent les citoyens. Il s'agit de lois « quasi constitutionnelles » qui ont généralement préséance sur d'autres lois.

ACCÈS À L'INFORMATION



La Loi fournit au public un processus lui permettant d'avoir accès à la plupart des documents en la possession ou relevant des organismes publics. Ainsi, le public a généralement le droit d'accéder à tout document détenu par un organisme public. Ce droit est toutefois visé par un certain nombre d'exceptions spécifiques; la plupart de ces exceptions servent à protéger les droits concernant la vie privée des individus, à permettre aux représentants élus de rechercher et d'élaborer des politiques, et à assurer le bon fonctionnement du gouvernement. Les tribunaux de partout au pays, incluant même la Cour suprême du Canada, considèrent que l'accès à l'information doit être la norme; les exceptions prévues doivent donc être interprétées rigoureusement pour allouer le plus grand accès possible aux documents gouvernementaux.

Pour obtenir un document d'un organisme public, il faut en faire la demande par écrit et acheminer celle-ci à l'organisme public duquel on souhaite obtenir l'information.

À la réception d'une demande d'accès à l'information, l'organisme public a le devoir de trouver tous les documents éclairants pour la demande. Il doit ensuite examiner ces documents pour déterminer s'ils peuvent être divulgués, en tout ou en partie, en vertu de la Loi. Les organismes publics ont 30 jours pour répondre à une demande.

Si la réponse n'est pas reçue dans le délai imposé par la Loi, ou si la réponse reçue n'est pas satisfaisante, le requérant peut demander à la commissaire à l'information et à la protection de la vie privée de réviser la décision.

PROTECTION DE LA VIE PRIVÉE

La Partie II de la Loi définit les règles que doivent respecter les organismes publics concernant la collecte des renseignements personnels, la manière dont ces renseignements peuvent être utilisés lorsqu'ils ont été colligés, ainsi que les circonstances permettant la divulgation de ces renseignements à des tiers (qu'il s'agisse d'autres organismes publics ou de citoyens). Elle établit aussi un mécanisme permettant aux individus de consulter leurs propres renseignements personnels qui sont détenus par un organisme gouvernemental et de demander des corrections, s'il y a lieu.

De plus, cette partie de la Loi exige que les organismes publics maintiennent des mesures de sécurité adéquates pour veiller à ce que les renseignements personnels dont ils font la collecte ne puissent être consultés par des personnes non autorisées.

LE RÔLE DE LA COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE

Le Commissariat à l'information et à la protection de la vie privée a été créé afin d'instaurer un mécanisme indépendant de surveillance à l'égard des questions touchant l'application et l'interprétation de la Loi. La commissaire à l'information et à la protection de la vie privée a été nommée par le commissaire des TNO, sur la recommandation de l'Assemblée législative, pour un mandat de cinq ans. En tant que représentante indépendante, elle ne peut être destituée que pour un motif valable ou en raison d'un empêchement. Cela lui confère donc le pouvoir de formuler des commentaires librement et directement.

Le travail de la commissaire à l'information et à la protection de la vie privée comporte quatre grands volets :

1. La commissaire répond aux demandes de révision qui concernent les décisions prises par les organisms publics à l'égard des demandes d'accès à l'information; elle formule aussi des recommandations auprès de ces organismes.
2. La commissaire répond aux plaintes formulées par des personnes qui croient que leur vie privée n'a pas été respectée par un organisme public; elle formule aussi des recommandations auprès de ces organismes.
3. La commissaire conseille les organismes publics à l'égard des lois, des politiques ou des pratiques pouvant avoir une incidence sur le droit d'accès à l'information ou le droit à la vie privée des citoyens.

4. La commissaire informe et éduque la population à l'égard des droits relatifs à l'information, y compris le droit d'accès à l'information et le droit à la vie privée.

Lorsqu'il y a contestation à la suite d'une réponse à une demande visant l'accès à de l'information gouvernemetale, le rôle de la commissaire est d'examiner, de manière indépendante et non partisane, les décisions prises par les organismes publics.

Lorsque la commissaire reçoit une demande de révision, elle prend des mesures pour déterminer quels documents sont concernés ainsi que pour obtenir une explication de la part de l'organisme public afin de connaître le processus et les raisons qui ont mené à la décision. Le requérant et les tiers dont les renseignements sont visés par la demande ont eux aussi l'occasion d'exposer leur point de vue. Dans presque tous les cas, la commissaire reçoit une copie de tous les documents éclairants dans leur version originale ainsi que dans la version soumise au requérant; elle peut ainsi voir quelles pages ont été divulguées, quelles pages ne l'ont pas été, et quels mots ou paragraphes ont été cachés par l'organisme public en répondant à la demande. La commissaire tient donc compte du point de vue des parties concernées, des documents eux-mêmes et des dispositions de la Loi afin de rédiger un rapport accompagné de recommandations. En règle générale, la commissaire n'a pas le pouvoir d'obliger les organismes publics à divulguer ou à cacher des renseignements, mais elle a l'obligation de formuler des recommandations.

Le responsable de l'organisme public doit ensuite prendre une décision finale, soit d'accepter les recommandations, de rejeter

les recommandations, ou encore de prendre d'autres mesures qu'il juge appropriées à la lumière des recommandations formulées par la commissaire. Si la personne qui voulait accéder à ces renseignements n'est pas satisfaite de la décision de ce responsable, elle peut ensuite faire appel à la Cour suprême des Territoires du Nord-Ouest, qui tranchera définitivement la question.

La commissaire a aussi le pouvoir de mener un examen et de formuler des commentaires et des recommandations dans les cas où une personne estime que ses renseignements personnels ont été recueillis, utilisés ou divulgués de manière inappropriée. Ainsi, lorsqu'elle reçoit une plainte pour atteinte à la vie privée, la commissaire fait enquête pour déterminer ce qui s'est passé exactement, comment cela s'est produit, et s'il y a effectivement eu atteinte à la vie privée. Que la plainte soit fondée ou non, la commissaire produit un rapport s'accompagnant presque toujours de commentaires et de recommandations visant à améliorer les politiques et les procédures de manière à éviter de futures atteintes à la vie privée. Les recommandations de la commissaire sont communiquées au responsable de l'organisme public concerné, qui doit alors décider s'il les accepte ou non. Par contre, un plaignant ne dispose du droit d'appel de la décision d'un organisme public lorsqu'il s'agit d'une plainte pour atteinte à la vie privée.

BILAN DE L'ANNÉE

L'exercice 2012-2013 a une fois de plus été chargé pour la commissaire à l'information et à la protection de la vie privée. Au cours des 12 mois qui se sont écoulés du 1er avril 2012 au 31 mars 2013, le Commissariat a ouvert 16 dossiers, soit un peu moins que durant l'exercice précédent. Ces dossiers se répartissent dans les catégories suivantes :

a)	Plaintes pour atteinte à la vie privée	4
b)	Demandes de révision – Décisions relatives à l'accès à l'information	1
c)	Acheminement erroné de télécopies contenant des renseignements médicaux	3
d)	Retards	1
e)	Demandes de révision – Évaluation des droits	5
f)	Dossiers médicaux trouvés	1
g)	Administration	1

Toutes les demandes de révision concernant l'évaluation des droits ont été traitées dans le cadre d'un processus informel; ainsi, aucun rapport n'a été rédigé, et aucune recommandation n'a été formulée. Deux des trois cas liés à un acheminement erroné de télécopies contenant des renseignements médicaux personnels ont été déclarés par

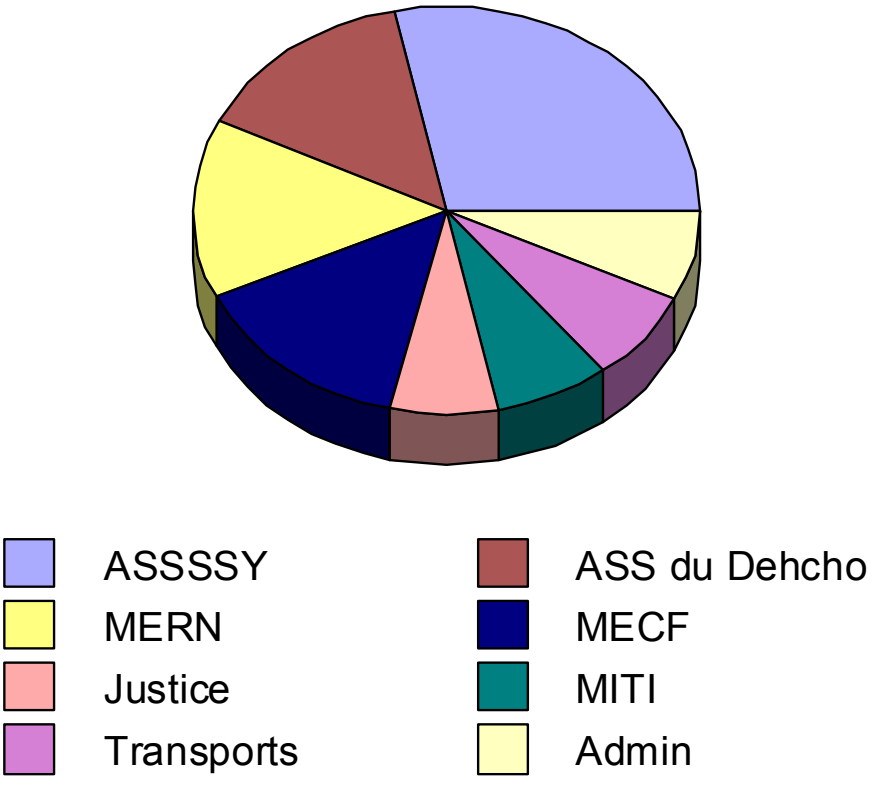
l'administration de santé fautive. Puisque, dans ces deux cas, l'organisme public a décelé l'erreur rapidement et a pris des mesures proactives pour corriger la situation, la commissaire a choisi de ne pas rédiger de rapports en bonne et due forme. Le dossier qui concernait un retard a également été traité très rapidement par la commissaire; encore là, elle a préféré ne pas rédiger un rapport complet, ni formuler de recommandations officielles. Elle a toutefois fait parvenir à l'organisme public fautif une longue missive exposant ses préoccupations ainsi que ses suggestions pour corriger le problème à la source. Enfin, dans un cas, un citoyen a rapporté un document qu'il avait trouvé dans une ruelle du centre-ville de Yellowknife et qui contenait des renseignements médicaux personnels d'une autre personne. Grâce aux renseignements contenus dans le document, la commissaire a pu communiquer avec la personne concernée pour l'informer que le document avait été retrouvé et pour lui demander si elle avait eu des craintes à cet égard. N'ayant pas eu de nouvelles de la personne concernée, la commissaire a conclu, d'après le contenu du document, que celui-ci avait probablement été égaré par la personne même. En effet, rien ne laissait indiquer que le document avait été égaré par un fournisseur de soins de santé. Par conséquent, la commissaire a choisi de ne prendre aucune autre mesure dans ce dossier.

Plusieurs organismes publics ont été impliqués dans les dossiers qui ont été présentés à la commissaire en 2012-2013 :

Administration des services de santé et des services sociaux de Yellowknife	4
Administration des services de santé et des services sociaux du Dehcho	2
Ministère de l'Environnement et des Ressources naturelles	2
Ministère de l'Éducation, de la Culture et de la Formation	2
Ministère de la Justice	1
Ministère de l'Industrie, du Tourisme et de l'Investissement	1
Ministère des Transports	1
Ministère de l'Exécutif	1

Durant l'exercice 2012-2013, la commissaire à l'information et à la protection de la vie privée a fomulé 12 recommandations relatives à des demandes de révision de décisions.

Organismes publics impliques



RECOMMANDATIONS RELATIVES AUX DEMANDES DE RÉVISION

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION Nº 12-105

« Quiconque désire faire respecter son droit le plus strict à la protection de ses renseignements médicaux personnels devrait pouvoir le faire en toute liberté. Je ne peux imaginer aucune situation qui mériterait qu'un employé soit réprimandé pour avoir formulé une demande ou une plainte à ce sujet. »

Le plaignant, qui était également un employé de l'organisme visé, a affirmé que ses renseignements médicaux personnels avaient été utilisés ou divulgués de manière inappropriée par l'Administration des services de santé et des services sociaux de Beaufort-Delta (ASSSSBD) après avoir reçu de l'assistance médicale de la part de cet organisme. Il a indiqué que des documents liés à son rendez-vous médical avaient été utilisés par la suite, sans son consentement, dans le contexte d'une instance disciplinaire relative à son emploi. Lorsqu'il a voulu demander des explications au directeur général au sujet de cette apparente atteinte à la vie privée, le plaignant s'est vu répondre qu'il devait respecter la voie hiérarchique et ainsi s'adresser à sa supérieure immédiate. On l'a également menacé de mesures disciplinaires s'il persistait à vouloir demander des explications au directeur général.

Deux enquêtes internes – une informelle et l'autre formelle – ont subséquemment été menées pour vérifier les allégations du plaignant. Dans les deux cas, il a été déterminé qu'il n'y avait eu

aucune atteinte à la vie privée du plaignant; cela dit, le plaignant n'a jamais été interrogé par les enquêteurs, et les conclusions ne lui ont pas été détaillées. Une copie du rapport d'enquête officiel a été remise non seulement au plaignant, mais aussi – malencontreusement – à sa supérieure immédiate ainsi qu'à plusieurs autres personnes au sein de l'organisme, possiblement parce que le rapport a été versé dans le dossier d'employé du plaignant.

« Rien ne pouvait justifier que le rapport d'enquête, celui-là même qui avait été préparé après que le patient se fut inquiété de la confidentialité de son dossier médical, soit transmis à toute autre personne que le directeur général et le patient concerné. »

L'organisme public a nié que des renseignements tirés du dossier médical du plaignant ont été utilisés dans le cadre de l'instance disciplinaire en question. Les renseignements fournis lors de cette instance disciplinaire auraient simplement été le fruit d'observations, et les conclusions présentées seraient découlées de ces observations et d'une connaissance générale d'autres faits.

La commissaire a finalement déterminé que la supérieure immédiate n'a jamais consulté directement le dossier médical du plaignant; elle a toutefois fait remarquer que, dans l'éventualité où des renseignements concernant l'état de santé du plaignant auraient été connus par la supérieure immédiate uniquement en vertu de son rang hiérarchique au sein de l'organisme, l'utilisation de ces renseignements dans le cadre d'une instance, disciplinaire ou autre, aurait été répréhensible sans le consentement du plaignant. Dans le présent cas, cependant, le plaignant a manifestement fourni lui-même à sa supérieure une lettre de son médecin à l'égard de son état de santé, et sa supérieure a

simplement déduit le reste d'après les circonstances. Au bout du compte, il n'y avait pas assez de preuves permettant de conclure que les renseignements médicaux personnels du plaignant ont été utilisés de manière inappropriée.

En abordant la question des circonstances, la commissaire a commenté la vaste distribution du rapport d'enquête interne, et particulièrement le fait qu'on ait jugé nécessaire de consigner une plainte relative à une atteinte à la vie privée dans le dossier d'un employé. La commissaire a fermement condamné le fait qu'on ait associé une plainte privée à la situation d'emploi d'une personne. Lorsque le plaignant a demandé au directeur général de se pencher sur ce qu'il considérait être une atteinte à sa vie privée, il ne l'a pas fait en tant qu'employé, mais en tant que simple citoyen. Rien ne pouvait justifier le fait que le rapport soit placé dans son dossier d'employé, ni même que la plainte soit connue de quelque autre personne dans son lieu de travail. Il ne s'agissait aucunement d'une question liée à son emploi.

La commissaire a recommandé à l'ASSSSBD qu'elle prenne des mesures pour revoir ses politiques et procédures concernant la confidentialité des dossiers médicaux de ses employés ainsi que les circonstances permettant l'utilisation des renseignements contenus dans ces dossiers. La commissaire a aussi recommandé la création de politiques claires afin de permettre à un patient qui est également un employé de déposer une plainte pour atteinte à la vie privée, sans craindre pour sa situation d'emploi, lorsqu'il

estime que ses renseignements médicaux personnels sont utilisés ou divulgués de manière inappropriée.

Les recommandations ont été acceptées par l'ASSSSBD, qui s'est engagée à entreprendre des mesures afin de revoir ses politiques actuelles concernant les dossiers médicaux de ses employés et les circonstances permettant l'utilisation des renseignements qui y sont contenus. L'ASSSSBD s'est également engagée à élaborer des politiques énonçant clairement les droits des employés lorsqu'ils souhaitent déposer une plainte pour atteinte à la vie privée sans craindre d'être pénalisés ou de faire l'objet de mesures disciplinaires.

« Les citoyens ont le droit de savoir qui a accédé à leurs dossiers personnels et dans quel but. Si une administration des services de santé n'est pas en mesure de répondre à ces questions, c'est qu'il y a une faille dans le système. »

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-106

Un patient de l'ASSSSBD a déposé une plainte, alléguant que ses renseignements médicaux personnels avaient été compromis. Le plaignant était, comme dans le cas précédent, un employé de l'ASSSSBD. Il avait reçu des soins médicaux au service des urgences de l'hôpital d'Inuvik, et avait demandé à ce que l'accès à la version papier de son dossier médical soit restreint, car il ne voulait pas que ses collègues soient au courant de ses problèmes de santé. Le dossier physique a été protégé

sur-le-champ, mais le plaignant s'est par la suite inquiété de la possibilité que son dossier électronique ne soit pas protégé. Il a donc demandé qu'une vérification soit effectuée à cet égard, et cette vérification a révélé que son dossier électronique avait été consulté à 12 reprises par des membres du personnel médical, clinique et de bureau en dehors de la période où il a reçu des soins médicaux.

« À mon avis, ce sont les administrations des services de santé qui ont la responsabilité de prouver qu'un accès à un dossier médical personnel est légitime en vertu de la Loi. En laissant croire au plaignant qu'il doit justifier pourquoi il considère inappropriée la consultation ou la divulgation de ses renseignements médicaux personnels, on n'adopte tout simplement pas la bonne approche. »

Le système de dossiers électroniques mis en place à l'hôpital d'Inuvik tient compte du nombre de fois qu'un dossier est consulté et peut déterminer qui a accédé au dossier. Le système est également censé demander aux utilisateurs d'indiquer les raisons de l'accès. L'accès au système était contrôlé par l'utilisation de noms d'utilisateurs. Chaque employé s'était vu fournir un nom d'utilisateur unique, mais il était possible, dans certains cas, d'accéder au système en utilisant un nom d'utilisateur générique, comme « *emerg* » ou « *clinic* ».

Un examen du rapport de vérification a permis de confirmer que, pour la plupart des 12 fois où les renseignements du plaignant ont été consultés en dehors de la période de traitement, l'accès a eu lieu pour des raisons légitimes, notamment pour la facturation, l'enregistrement des soins d'urgence, l'envoi de données à la CSTIT, l'enregistrement d'une activité en laboratoire, ou tout autre motif clairement légitime associé à la santé ou aux soins du patient. Toutefois, dans plusieurs cas, aucun utilisateur précis n'a pu être identifié (l'utilisateur étant, dans ces cas, désigné sous le nom « *emerg* » ou « *clinic* »), et aucun motif n'a été consigné pour l'accès.

L'ASSSSBD a soutenu que la vérification, en soi, ne permettait pas de confirmer s'il y a eu utilisation ou divulgation inappropriée de renseignements médicaux personnels. De plus, elle a soutenu que même lorsqu'aucun utilisateur ou motif précis n'a pu être déterminé pour l'accès aux renseignements, rien ne pouvait laisser croire que ces renseignements ont été utilisés ou divulgués de manière inappropriée.

« Les administrations des services de santé se doivent de comprendre que tout accès non autorisé ou toute consultation injustifiée du dossier médical d'un patient, que les renseignements contenus dans le dossier soient ou non utilisés ou divulgués subséquemment, constitue une atteinte à la vie privée du patient. Il faut donc s'abstenir de consulter les dossiers des patients, à moins que ce ne soit pour un motif médical ou administratif. »

La commissaire a fait état de plusieurs préoccupations, particulièrement en ce qui concerne les cas où l'accès a été fait à partir d'un nom d'utilisateur générique plutôt qu'un nom d'utilisateur individuel, ainsi que ceux où aucune note n'a été laissée pour indiquer le motif de l'accès. Elle s'est aussi inquiétée du fait que l'ASSSSBD voulait que le plaignant ait la responsabilité de prouver l'accès injustifié à son dossier, alors que la Loi oblige clairement les organismes publics à veiller à la sécurité des dossiers. La commissaire a également mentionné que tout accès non autorisé ou toute consultation injustifiée du dossier d'un patient, que les renseignements contenus dans le dossier soient ou non utilisés ou divulgués subséquemment, constitue une atteinte à la vie privée du patient, particulièrement dans les petites collectivités où tout le monde se connaît. Enfin, tout accès à un dossier doit être considéré comme non autorisé et injustifié lorsque ce n'est pas pour un motif médical ou administratif. La commissaire a formulé six recommandations à ce sujet :

1. que l'ASSSSBD réalise une évaluation approfondie des répercussions sur la vie privée du système de dossiers

électroniques mis en place à l'hôpital d'Inuvik et prenne des mesures pour améliorer la sécurité et les contrôles du système en fonction des résultats de cette évaluation;

2. que des mesures soient prises pour retirer immédiatement du système tous les noms d'utilisateurs génériques et mots de passe associés;

3. que des mesures soient prises pour veiller à ce que tout accès au système s'accompagne d'une justification;

4. que l'ASSSSBD prépare et mette en œuvre, à l'intention de tous ses employés, une séance d'orientation obligatoire sur le sujet de la vie privée;

5. que des messages soient communiqués de manière continue aux employés pour leur rappeler l'importance de protéger la vie privée des patients lorsqu'ils doivent consulter leur dossier médical;

6. que des mesures soient prises immédiatement pour veiller à ce que le système fasse l'objet de vérifications aléatoires et régulières.

L'organisme public s'est montré en désaccord avec la conclusion de la commissaire selon laquelle il était du devoir de l'organisme public de prouver qu'il n'y a eu aucun accès non autorisé au dossier médical du plaignant pouvant constituer une infraction aux dispositions en matière de vie privée prévues par la Loi. Cela dit, l'organisme public a accepté l'entièreté des recommandations formulées.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-107

Une avocate représentant des requérants en vertu de la Convention de règlement relative aux pensionnats indiens a demandé à la commissaire de se pencher sur le délai pour obtenir les renseignements nécessaires afin de présenter et d'appuyer une demande auprès du ministère de l'Éducation. Elle a fourni plusieurs exemples de demandes d'accès à l'information pour lesquelles il avait fallu attendre au moins un an avant d'obtenir une réponse, soit une période beaucoup plus longue que les 30 jours prévus par la *Loi sur l'accès à l'information et la protection de la vie privée*.

« Cela dit, le gouvernement des Territoires du Nord-Ouest a le devoir, selon la Loi, de répondre aux demandes d'accès à l'information dans un délai de 30 jours ou, dans certaines situations particulières, dans un délai raisonnablement prorogé. »

Le ministère a reconnu avoir reçu un nombre croissant de demandes d'accès à l'information liées à la question des pensionnats. Entre 2005 et juillet 2011, il a reçu un total de 1 265 demandes et n'a pu répondre complètement qu'à 894 d'entre elles, ce qui laissait 371 demandes encore en suspens, dont certaines datant de 2005. Bien que certaines mesures aient été prises pour rationaliser les processus et embaucher plus de personnel de manière à réduire les délais de réponse, le ministère affichait encore un retard considérable.

La commissaire a fait remarquer que la Loi prévoit un délai de réponse de 30 jours. Elle a également souligné qu'il existe des dispositions dans la Loi permettant une prorogation de délai dans certaines circonstances, et que le ministère n'a pas semblé suivre les étapes indiquées dans la Loi pour les prorogations. Elle a toutefois noté que le ministère semblait travailler avec ardeur et de bonne foi pour répondre à l'ensemble des demandes reçues.

La commissaire a formulé les recommandations suivantes à l'intention du ministère de l'Éducation, de la Culture et de la Formation ainsi que du service Archives des TNO :

« Il faut veiller à ce qu'il y ait suffisamment d'effectifs s'occupant de répondre aux demandes d'accès à l'information pour s'assurer que, dans la plupart des cas, on respecte le délai de 30 jours. »

a) qu'ils embauchent assez de personnel pour rattraper le retard actuel dans un délai de 90 jours suivant la date du rapport de la commissaire;

b) qu'ils veillent, de manière continue, à ce qu'il y ait au sein du ministère ou du service Archives des TNO suffisamment d'employés à temps plein qui s'occupent exclusivement de répondre aux demandes d'accès à l'information;

c) qu'ils prennent des mesures pour s'assurer que les procédures appropriées sont respectées lorsqu'il y a prorogation de délai pour une réponse;

d) que le ministère se rapporte deux fois par mois au Commissariat à l'information et à la protection de la vie privée jusqu'à ce que le retard soit complètement rattrapé.

Les recommandations ont été acceptées. Dans les mois qui ont suivi la publication du rapport, le ministère a réussi à rattraper une bonne partie de son retard; il y a actuellement beaucoup moins de vieux dossiers encore en suspens.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-108

Un consultant a demandé une copie de l'entente provisoire sur la chasse au caribou de la toundra, un accord intergouvernemental survenu entre le ministère de l'Environnement et des Ressources naturelles (MERN) du gouvernement des TNO et la Première Nation des Dénés Yellowknives (PNDY) au sujet de la gestion des troupeaux de caribous. Cette entente avait soulevé la controverse, et beaucoup de citoyens s'y étaient intéressés.

« En tant que gouvernement démocratique exerçant ses activités au Canada, la PNDY devra, à un moment donné, se résigner à acquiescer aux demandes d'accès à ses documents. Pour l'instant, cependant, la PNDY n'est pas assujettie aux règles de l'accès à l'information qui sont définies par la *Loi sur l'accès à l'information et la protection de la vie privée.* »

Le MERN a refusé de divulguer toute partie de l'entente, affirmant qu'une divulgation pourrait vraisemblablement porter atteinte aux relations entre le gouvernement des TNO et la PNDY.

Lorsqu'elle a été consultée, la PNDY s'est clairement et vigoureusement objectée à ce que toute partie de l'entente soit divulguée, même celles qui donnent simplement une mise en contexte. Le ministère a également souligné qu'il avait promis à la PNDY de garder l'entente confidentielle à moins que la PNDY accepte de la divulguer en tout ou en partie. Le requérant, pour sa part, a soutenu que l'entente concernait une importante question d'intérêt public et que même si la PNDY ne souhaitait pas en diffuser le contenu, rien ne laissait croire qu'une divulgation

pourrait entraîner des conséquences négatives. Le requérant a ajouté que la gestion et la conservation de la faune étaient des questions d'ordre public qui méritaient d'être ouvertes aux citoyens; le fait qu'elles puissent constituer un sujet controversé ou délicat du point de vue politique ne justifiait pas la non-divulgation de l'entente.

« Ce qu'il faut se demander, c'est si la diffusion de l'entente risque vraisemblablement de nuire aux relations entre les deux gouvernements. D'après les commentaires formulés par la PNDY, j'en conclus que la diffusion porterait effectivement atteinte aux relations entre les deux gouvernements dans ce cas. »

La commissaire a rappelé que la *Loi sur l'accès à l'information et la protection de la vie privée* a pour objectif de favoriser la démocratie, et que toute exception au droit d'accès à l'information doit faire l'objet d'une interprétation rigoureuse. Elle a également fait remarquer que la PNDY est une organisation autochtone visée par l'article 16 de la Loi. Cet article donne aux organismes publics le pouvoir discrétionnaire de refuser l'accès à certains documents dont la divulgation risquerait vraisemblablement de nuire aux relations entre le gouvernement des TNO et une organisation autochtone.

Dans le cadre de son processus d'examen, la commissaire s'est adressée directement à la PNDY pour connaître son point de vue. La PNDY a maintenu son opposition ferme à la divulgation de l'entente, craignant qu'une divulgation puisse susciter la controverse, lui attirer des critiques ou ouvrir la porte à des enquêtes.

La commissaire a indiqué que ces craintes ne suffisaient pas à justifier la non-divulgation du contenu d'un document par un organisme public; toutefois, la PNDY n'est pas un organisme public au sens de la Loi et, par conséquent, elle n'est pas assujettie aux mêmes règles. Puisque la PNDY a exprimé une forte objection à

l'idée de la divulgation, la commissaire a conclu que la diffusion de l'entente risquerait vraisemblablement de nuire aux relations entre les deux gouvernements et que le refus de divulguer les détails de l'entente était acceptable dans ce cas.

La commissaire a formulé les recommandations suivantes :

a) que le MERN analyse pleinement sa position à l'égard de la divulgation de l'entente, en gardant en tête que la Loi oblige normalement la divulgation des documents publics, sauf encas d'exceptions – et le cas échéant, les exceptions doivent faire l'objet d'une interprétation rigoureuse;

b) que le MERN envisage attentivement, en particulier, la possibilité de divulguer les parties de l'entente qui sont déjà connues du public, y compris les parties qui font état de faits historiques et qui offrent uniquement une mise en contexte.

Le ministère, après avoir tenu des discussions avec les chefs de la PNDY, a déterminé que la relation entre les deux gouvernements (le gouvernement des TNO et le gouvernement des Premières Nations dénées d'Akaitcho) serait négativement affectée par la divulgation de l'entente, ce qui compromettrait de futures négociations, y compris concernant les revendications territoriales et les ententes de coopération sur la gestion des caribous. Le ministère a donc conclu que la perte de confiance entre les deux parties serait plus dommageable que le manque de transparence à l'égard des citoyens dans ce cas précis. Par conséquent, le ministère a exercé son pouvoir discrétionnaire et a refusé de divulguer le contenu de l'entente.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-109

Le plaignant, un employé du gouvernement des TNO atteint de plusieurs déficiences physiques et mentales, était d'avis que l'Administration des services de santé et des services sociaux de Yellowknife (ASSSSY) et son médecin personnel avaient divulgué de manière inappropriée ses renseignements médicaux personnels. La situation du plaignant exigeait que ce dernier ait droit à des accommodements en milieu de travail, et il avait été convenu qu'il se soumette à une évaluation psychiatrique pour faciliter le choix des accommodements qui répondraient le mieux à ses besoins. Le plaignant a affirmé qu'il avait reçu l'assurance que les renseignements détenus par le psychiatre ne seraient pas communiqués à son employeur. Malgré cela, le médecin aurait envoyé à l'employeur une lettre portant sur son évaluation et y aurait joint une copie intégrale du rapport psychiatrique.

« La Loi sur l'accès à l'information et la protection de la vie privée régit le droit d'accès à l'information que possèdent les citoyens; les dispositions contenues dans la Loi prévalent donc contre les simples promesses de confidentialité. »

Le médecin, pour sa part, a indiqué qu'il avait examiné le rapport psychiatrique en compagnie du plaignant et qu'ils avaient tous deux convenu de remettre le rapport à l'employeur. Le médecin a reconnu avoir préparé une lettre à l'intention de l'employeur et joint une copie du rapport psychiatrique à cette lettre. Il a cependant nié que cette lettre a été remise à l'employeur par une personne travaillant à son cabinet. Cela dit, même si la lettre a été remise à l'employeur par

l'ASSSSY, celle-ci a soutenu qu'elle avait obtenu le consentement écrit du plaignant pour la divulgation des renseignements. Elle n'avait pas de preuve attestant l'envoi de la lettre, mais un employé s'est rappelé que le plaignant s'était présenté au cabinet, qu'il avait lu la lettre et le rapport, puis qu'il avait signé une formule de consentement afin que les deux documents soient transmis à l'employeur. L'organisme public a indiqué que c'était probablement le plaignant lui-même qui avait remis la lettre à son employeur.

« Le serment de confidentialité vise à empêcher un employé de discuter des renseignements personnels d'un patient à l'extérieur du lieu de travail; il ne vise pas la question de l'accès non autorisé ou injustifié aux dossiers médicaux personnels. Il s'agit là de deux choses différentes. »

Peu importe la manière dont elle a été transmise, toutes les parties ont convenu que la lettre et la pièce jointe avaient bel et bien été remises à l'employeur du plaignant. Le plaignant a toutefois eu le temps de la récupérer intacte avant qu'elle ne soit ouverte et lue.

La commissaire a statué qu'il n'y avait pas réellement eu de divulgation, étant donné que la lettre a été récupérée auprès de l'employeur avant même d'avoir été lue. Elle s'est toutefois inquiétée du fait que l'organisme public n'était pas, dans ce cas, en mesure de confirmer comment ni quand la lettre a quitté le cabinet. Elle a également ajouté que la formule de consentement signée par le plaignant était incomplète, le nom et l'adresse du destinataire visé n'étant pas indiqués. Elle a fait remarquer qu'il était du devoir de l'organisme public de s'assurer d'avoir un consentement adéquat pour la divulgation de renseignements; dans le cas de dossiers médicaux de nature délicate, un consentement verbal ou apparent ne suffit pas. De plus, la commissaire a émis des réserves quant au fait que le médecin a

décrit l'information contenue dans le rapport de consultation comme des « questions de fait » alors que le rapport contenait une quantité importante de renseignements médicaux historiques de nature privée. Il semblait également que le médecin n'ait pas reconnu la nature délicate de la situation ni l'importance d'enregistrer les discussions entourant le consentement verbal : en effet, la commissaire a remarqué qu'aucune note n'avait été versée dans le dossier du plaignant concernant sa discussion avec le médecin.

« Puisque c'est l'organisme public qui doit rendre compte de la collecte, de l'usage et de la divulgation de renseignements personnels, c'est aussi lui qui doit s'assurer que les formulaires [de consentement] sont remplis de manière complète et adéquate. L'organisme public ne peut pas simplement se fier à de simples directives verbales lorsqu'il est question de renseignements médicaux personnels. »

La commissaire a formulé des recommandations pour :

a) qu'un système et des procédures spécifiques soient mis en place afin de gérer les consentements visant la divulgation de renseignements médicaux; une liste de vérification pourrait entre autres aider les employés de soutien à s'assurer que chaque étape du processus est respectée, que tous les renseignements requis sont consignés sur les formulaires de consentement, et qu'il y a suffisamment d'espace pour permettre aux patients de prendre des notes ou de formuler des instructions précises;

b) que lorsque les patients demandent la divulgation de renseignements médicaux personnels à des tiers (comme des employeurs ou des compagnies d'assurances), les médecins soient encouragés à verser des notes dans le dossier de leurs patients afin de pouvoir confirmer ultérieurement qu'une discussion a bel et bien eu lieu concernant la divulgation et,

le cas échéant, que des instructions particulières ont été reçues du patient.

Les recommandations ont été acceptées.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-110

« Lorsqu'un médecin fait face à quelqu'un qui lui parle, sans raison valable, des renseignements médicaux privés d'une autre personne, il est de son devoir de mettre fin à la conversation le plus rapidement possible. »

Le plaignant avait des antécédents de problèmes de santé mentale et devait prendre des médicaments à cet égard; il était d'ailleurs toujours en traitement. Un jour, il est allé voir son médecin, qui lui a raconté que des membres de sa famille étaient allés le rencontrer pour discuter de son comportement et exprimer leurs inquiétudes au sujet de son état de santé mentale. Ceci a été confirmé lors de discussions tenues avec ces mêmes membres de la famille, qui ont admis au plaignant avoir discuté de son comportement avec son médecin. Cependant, aucune note n'a été laissée dans le dossier médical du plaignant pour confirmer que le médecin avait bel et bien discuté de la question avec des membres de la famille.

L'ASSSSY a confirmé que le médecin avait effectivement rencontré des membres de la famille du plaignant, mais a nié que cette rencontre concernait le plaignant. L'ASSSSY a plutôt indiqué

que le médecin a rencontré ces personnes pour leur prodiguer des soins médicaux.

La commissaire a conclu, à la lumière des renseignements qui lui ont été soumis par toutes les parties, qu'il y a vraisemblablement eu des discussions au sujet du plaignant entre le médecin et des membres de la famille. Toutefois, rien ne pouvait prouver que le médecin a amorcé ces discussions ou qu'il y a participé pour une autre raison que de suggérer que le plaignant se fasse traiter. La commissaire a noté que même si un médecin ne peut être tenu responsable des propos tenus par un patient, il demeure responsable de sa propre réaction. Dans le cas présent, il n'y avait tout simplement pas assez de preuves pour conclure que le médecin a fait autre chose que de répondre aux inquiétudes des membres de la famille et suggérer que le plaignant aille demander de l'aide. Par conséquent, la commissaire a dé terminé qu'il n'y a eu aucune atteinte à la vie privée, et elle n'a donc formulé aucune recommandation. Pour sa part, l'organisme public n'a pas répondu aux commentaires émis par la commissaire.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-111

Un requérant voulait accéder à des documents du ministère de l'Industrie, du Tourisme et de l'Investissement en lien avec les doubles de certificats et les certificats de remplacement émis par le ministère dans le cadre du programme Diamants canadiens certifiés du gouvernement des TNO. Après avoir mené des consultations auprès de tiers, l'organisme public a divulgué le nombre total de certificats de remplacement émis ainsi que le nom de certaines des entreprises qui en ont demandé. L'organisme a toutefois refusé de divulguer le nom de certaines autres entreprises en affirmant que cette divulgation risquerait vraisemblablement d'entraîner des pertes ou des gains indus sur le plan financier, ou encore de porter atteinte à la position concurrentielle de ces entreprises. L'organisme a aussi refusé de nommer les individus (par opposition aux entreprises) qui ont reçu des doubles de certificats, indiquant qu'il s'agirait là d'une atteinte déraisonnable à la vie privée de ces personnes. Enfin, l'organisme a refusé de divulguer le nombre réel de doubles de certificats délivrés à chaque entreprise, de même que les critères sur lesquels s'est appuyée l'émission des doubles.

La commissaire a reconnu que la divulgation du nom des deux personnes qui ont reçu des doubles de certificats était à éviter, car cela constituerait une atteinte déraisonnable à la vie privée de

ces personnes. Cela dit, même si ces noms devaient être cachés, il n'y avait aucune raison de ne pas expliquer publiquement, de manière sommaire, les raisons derrière l'émission des doubles.

La commissaire n'était pas d'accord avec la décision du ministère de refuser la divulgation du nom de deux entreprises qui n'ont pas pris part aux consultations menées par le ministère auprès de tiers. Le fait que des entreprises se livrent à l'achat, à la vente et au commerce de diamants ne constitue pas de l'information protégée en vertu de la Loi. Par ailleurs, la commissaire n'a pu trouver aucune preuve montrant que la divulgation des renseignements demandés spécifiquement par le requérant porterait atteinte aux intérêts commerciaux de l'une ou l'autre des entreprises visées.

« En ne divulguant pas le nom des personnes ayant demandé les certificats, on enlève tout renseignement personnel de l'équation : il n'y a donc plus aucune raison de ne pas donner au requérant l'information voulue. »

En supposant que le requérant accepterait de recevoir de l'information plutôt que des documents, la commissaire a recommandé que l'organisme public divulgue le nom de toutes les entreprises qui ont demandé ou reçu des doubles de certificats, de même que le nombre de doubles émis à chaque entreprise et individu ainsi que les critères sur lesquels s'est appuyée l'émission des doubles. La commissaire recommande toutefois de ne pas de divulguer le nom des individus concernés.

Les recommandations ont été acceptées.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-112

L'employeur du plaignant voulait que celui-ci obtienne un pronostic écrit de son médecin. Dans cette perspective, le plaignant a signé la section de consentement du formulaire de demande de pronostic médical présentée par un employé, qu'il a présenté à son médecin avec une copie d'une lettre de son employeur indiquant les renseignements demandés. Cette lettre était adressée au plaignant. Des copies de celle-ci avaient aussi été envoyées à diverses personnes du service des ressources humaines de l'employeur. Dans le formulaire, le consentement était formulé comme suit :

> *J'autorise par la présente le professionnel de la santé à communiquer les renseignements à moi-même et (ou) au gouvernement des Territoires du Nord-Ouest.*

Le plaignant avait compris que son médecin remplirait le formulaire et le lui remettrait pour qu'il le transmette à son employeur. Or, le médecin a plutôt transmis à l'employeur le formulaire rempli qui contenait le consentement de l'employé, accompagné d'une lettre renfermant un certain nombre d'autres détails d'ordre médical. En outre, le médecin a choisi d'envoyer des doubles du formulaire et de sa lettre à toutes les personnes du

« Dans ce cas, le consentement fourni par le plaignant était équivoque. En effet, en signant le formulaire, le plaignant a consenti à ce que les renseignements liés au pronostic soient communiqués à lui-même et (ou) au gouvernement des Territoires du Nord-Ouest. »

service des ressources humaines qui avaient reçu une copie de la lettre adressée par l'employeur au plaignant.

L'organisme public était d'avis que le plaignant avait consenti à ce que ses renseignements personnels soient communiqués au gouvernement des TNO et que cela était suffisant pour autoriser la communication de ces renseignements à toutes les personnes qui avaient reçu une copie conforme du rapport.

« Le rapport du médecin aurait dû être remis uniquement au superviseur du plaignant. Ce n'est pas une question d'étiquette : c'est la loi qui l'exige. En effet, les organismes publics et leurs employés n'ont pas le droit d'utiliser ou de divulguer les renseignements personnels d'autrui, sauf dans les cas prévus par la Loi. »

La commissaire a observé que le formulaire de consentement sur lequel s'appuyait l'organisme public était équivoque et prêtait à une très large interprétation. La locution « et (ou) » rendait le consentement flou si l'on n'insistait pas d'une quelconque façon sur l'un de ses deux éléments. De plus, le « gouvernement des Territoires du Nord-Ouest » est une entité très vaste. Par ailleurs, le consentement ne semblait pas autoriser la communication de renseignements autres que ceux figurant dans le formulaire en question.

La commissaire a conclu qu'il y avait eu violation de la vie privée du plaignant, en particulier en conséquence de la diffusion élargie du formulaire rempli par le médecin et de la lettre qui l'accompagnait.

La commissaire a recommandé :

1. que la section « consentement » du formulaire de demande de pronostic médical présentée par un employé du gouvernement des TNO soit révisée de manière :

a) à ce que la personne qui donne son consentement doive préciser à qui les renseignements peuvent être communiqués;

b) à ce que la locution « et (ou) » soit retirée du formulaire de consentement;

c) à préciser que le consentement ne s'applique qu'aux renseignements contenus dans le formulaire connexe, à moins que le patient n'autorise expressément le médecin à ajouter des renseignements additionnels qui pourraient être nécessaires;

2. que tous les travailleurs de la santé, en particulier les médecins, reçoivent davantage de formation ou, à tout le moins, d'information sur les circonstances dans lesquelles ils peuvent communiquer à des tiers des renseignements personnels sur la santé des patients;

3. que des pratiques et des procédures soient établies quant aux obligations des travailleurs de la santé lorsqu'ils obtiennent un consentement à la communication de renseignements personnels sur la santé, afin que le processus et le message concordent.

L'organisme public n'a pas accepté l'analyse faite par la commissaire. Il était d'avis que le formulaire de consentement signé par le plaignant était suffisant pour autoriser le médecin à répondre directement à l'employeur et que le médecin avait agi correctement. L'organisme public convenait que le consentement était équivoque, mais il ne pouvait pas conclure que le médecin avait agi de manière déraisonnable en fournissant une lettre séparée en plus du formulaire rempli. Pour lui, le fait de présenter à l'employeur le formulaire rempli et une lettre contenant des renseignements additionnels ne constituait pas une violation de la

vie privée du patient. De son point de vue, fournir un double du rapport du médecin à toutes les personnes qui avaient déjà reçu des copies conformes ne violait pas non plus la vie privée du patient parce que « le résultat était ultimement conforme à la fin pour laquelle les renseignements avaient été recueillis et réunis ».

En définitive, l'organisme public a accepté de transmettre au ministère des Ressources humaines la recommandation de la commissaire concernant le formulaire de demande de pronostic médical du gouvernement des TNO. Il a aussi accepté de transmettre au ministère de la Santé et des Services sociaux les recommandations concernant les pratiques et les procédures liées à l'obtention du consentement. Il n'a pas accepté de revoir ses propres pratiques en cette matière.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-113

Le plaignant souhaitait obtenir des renseignements sur la récolte de l'ours blanc aux TNO. Certains renseignements ont été fournis, mais l'organisme public a refusé de communiquer les coordonnées latitudinales et longitudinales relatives aux prises d'ours blancs, au motif que cela révélerait les endroits où l'on trouve ces animaux. L'ours blanc ayant été inscrit sur la liste des espèces en péril en vertu de la *Loi sur les espèces en péril* canadienne, le ministère était d'avis que la divulgation de ces

renseignements en particulier pourrait constituer une menace additionnelle à la survie de l'espèce. Le plaignant a soumis un certain nombre de faits scientifiques sur les populations d'ours blancs qui donnaient à penser que la divulgation des sites de prise d'ours blancs n'était pas susceptible de fournir aux chasseurs un quelconque avantage important ni d'accroître les probabilités que des ours blancs soient localisés. Le ministère a soumis des renseignements scientifiques tout aussi convaincants qui laissaient supposer exactement le contraire.

La commissaire a conclu que l'article 19 de la *Loi sur l'accès à l'information et la protection de la vie privée* des TNO confère aux organismes publics un pouvoir discrétionnaire de refuser de divulguer des renseignements dans les cas où la divulgation risquerait vraisemblablement de nuire à des formes de vie rares, en voie de disparition, menacées ou vulnérables, ou de nuire à leur protection. Les deux parties ont présenté des arguments convaincants, mais la commissaire a jugé que l'organisme public avait soulevé des préoccupations légitimes et raisonnables quant à la divulgation des renseignements demandés et qu'il avait bien fait de refuser de communiquer des données latitudinales et longitudinales précises sur les prises d'ours blancs. Aucune autre recommandation n'a été formulée.

Le ministre a pris acte des conclusions et les a acceptées.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 12-114

Le plaignant était un employé d'une administration des services de santé et des services sociaux (ASSSS) régionale, travaillant comme conseiller dans une petite localité. Ses préoccupations concernaient l'obligation qu'il avait de fournir à l'administration centrale des renseignements détaillés sur des patients lorsqu'il était appelé à intervenir lors d'incidents en dehors des heures normales de travail. Il s'opposait à devoir inscrire les noms et les adresses de ses clients sur les formulaires prescrits, parce que cela allait à l'encontre de son devoir professionnel de protéger la confidentialité de ses clients. Lorsqu'il a soulevé cette question, on lui a répondu que, faute de fournir tous les renseignements demandés dans ces formulaires, il ne serait pas rémunéré pour ses heures supplémentaires.

« Si le superviseur, dans ce cas, peut s'acquitter de ses fonctions de supervision sans connaître le nom et l'adresse des clients auprès desquels est intervenu le conseiller en dehors des heures normales de travail, ces renseignements ne devraient pas être requis ni communiqués. »

Dans les formulaires en question, le conseiller devait indiquer le nom et le numéro de téléphone de la personne qui avait demandé son intervention, le nom de l'employé, la date et l'heure de l'appel, ainsi que le nom, l'adresse et le numéro de téléphone du client, la raison de l'intervention, un résumé du problème, les mesures prises par l'employé, l'état courant de la situation et les mesures de suivi nécessaires.

L'ASSSS a fait valoir que le formulaire devait être rempli pour un certain nombre de raisons. D'abord, il y avait une obligation légale de consigner les incidents en matière de santé et d'inscrire ces informations sur la fiche du client, dans son dossier permanent. Le formulaire avait aussi une fonction de gestion du risque, dans la mesure où il permettait aux superviseurs d'exercer un examen et une surveillance des mesures prises par le personnel ainsi que d'assurer la continuité des soins et le suivi nécessaire, dans les délais requis et de la manière appropriée. Le formulaire servait aussi dans le cadre de l'évaluation des programmes, pour assurer des niveaux de dotation appropriés et des modèles de prestation des services adaptés à chaque collectivité. Enfin, le formulaire servait à assurer la rétribution exacte de tous les services fournis sur appel par l'employé. Le superviseur, dans ce cas, se trouve dans une autre collectivité, et ses contacts directs avec le client sont rares, voire inexistants.

« La protection de la vie privée transcende la confidentialité. Certes, le serment de confidentialité constitue un excellent point de départ – et un instrument nécessaire – pour éviter l'utilisation ou la divulgation indue de renseignements médicaux personnels, mais cet outil est loin d'être infaillible. La nature humaine étant ce qu'elle est, il serait présomptueux de se fier aveuglément au serment pour empêcher l'utilisation ou la divulgation inappropriée de renseignements personnels. »

L'ASSSS a fait valoir que tous ses employés ont fait un serment de confidentialité et connaissent l'importance de garder les renseignements des clients confidentiels. Elle a aussi souligné que le superviseur faisait partie du « cercle de soins » du client puisqu'il relève du même programme que le conseiller.

La commissaire n'était pas persuadée de la nécessité de transmettre à l'administration centrale des informations de nature à identifier les clients et à divulguer des renseignements personnels sur leur santé. Elle a souligné que l'un des 10 principes de protection de la vie privée était de recueillir, d'utiliser ou de

divulguer seulement le minimum d'informations nécessaires pour une fin particulière. Elle a conclu que, même s'il était approprié de consigner toutes les informations sur le formulaire pour satisfaire aux exigences légales de tenue de dossiers, il n'était pas véritablement justifié que tous ces renseignements soient communiqués à l'administration centrale à des fins administratives. Tout en reconnaissant que la continuité des soins est un but important, la commissaire estime que si l'administration centrale avait réellement besoin de ces renseignements pour atteindre ce but, elle demanderait aux employés communautaires de fournir ce genre de renseignements pour tous les patients, et non seulement pour ceux qui reçoivent des services après les heures normales de travail.

« Je ne suis pas convaincue qu'il est nécessaire pour le superviseur de connaître le nom et l'adresse d'un client afin de s'acquitter adéquatement de ses fonctions de supervision à l'égard d'un employé. Dans les rares cas où le nom et l'adresse d'un client seraient, pour une raison quelconque, nécessaires à la supervision d'un employé, ces renseignements pourront être obtenus à partir du dossier du client, sur une base individuelle et selon les besoins. »

La commissaire a recommandé :

a) que l'ASSSS cesse immédiatement d'obliger les conseillers à fournir le nom et l'adresse des clients aux fins de la production de rapports sur les services fournis après les heures normales de travail, et qu'elle modifie ses formulaires de manière à ne recueillir que le minimum d'informations nécessaires pour permettre au superviseur de remplir les responsabilités liées à ses fonctions;

b) que l'ASSSS cesse d'utiliser l'expression « cercle de soins » pour justifier l'utilisation et la divulgation de renseignements personnels sur la santé, au moins jusqu'à ce qu'une définition raisonnable de cette expression ait été établie en

fonction de ce que le patient interpréterait comme étant le « cercle de soins » médical dans une situation particulière.

La première des deux recommandations a été acceptée. L'ASSSS a toutefois refusé d'accepter la recommandation relative à l'expression « cercle de soins ».

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 13-115

Le plaignant avait reçu par courriel des renseignements médicaux personnels de nature délicate qui avaient été transmis par télécopieur et qui concernaient un étranger. La télécopie avait été envoyée par la clinique de soins primaires de Yellowknife au moyen de la fonction de « numérisation et envoi par courriel » d'un photocopieur. Quelques minutes plus tard, le plaignant avait reçu une deuxième télécopie de la clinique lui demandant de détruire le courriel précédent.

En réponse à la plainte, la clinique de soins primaires de Yellowknife a expliqué que le plaignant était un de ses patients, avec qui elle ne pouvait communiquer que par courriel. Le patient n'avait pas de ligne téléphonique terrestre ni de téléphone cellulaire, mais il avait une connexion Internet et avait demandé

à la clinique de lui écrire à son adresse courriel personnelle lorsqu'elle devait communiquer avec lui. Cela ne représentait pas pour la clinique un moyen courant de communiquer avec les patients, mais elle l'utilisait pour accommoder ce patient en particulier. L'envoi de la télécopie à la mauvaise personne était, selon la clinique, dû à une erreur humaine ou technique, mais aucune autre explication n'a été donnée. Par suite de cette plainte, la clinique a cessé de communiquer avec le plaignant au moyen de la fonction « numérisation et envoi par courriel ».

« Nous apprenons de nos erreurs. Il est donc important que les organismes publics puissent expliquer comment une erreur s'est produite afin d'adopter des mesures pour éviter qu'elle ne se répète. La solution qui consiste à simplement cesser d'utiliser le moyen de communication en cause n'est pas nécessairement bonne, particulièrement à une époque où, comme mentionné précédemment, le public communique de plus en plus par voie électronique. »

La commissaire a souligné que, dans tout ce qui comporte une intervention humaine, il existe un risque d'erreur. Elle a aussi reconnu que la clinique avait immédiatement constaté son erreur et fait ce qu'elle avait pu pour récupérer les renseignements envoyés au mauvais endroit. Elle était toutefois préoccupée de constater que la clinique ne possède pas, à l'ère des télécommunications, de politique encadrant l'utilisation des moyens non conventionnels de communiquer avec les patients. Si un patient consent à ce que l'on communique avec lui par courriel, ce moyen de communication doit être une option viable; pour ce faire, des politiques et des procédures doivent encadrer son utilisation.

La commissaire était aussi préoccupée par le fait que la clinique ne puisse pas fournir plus de détails sur l'impair ni expliquer comment les renseignements d'un tiers avaient pu être envoyés au plaignant, autrement qu'en invoquant « l'erreur humaine ».

Faute de cerner la cause véritable, on ne peut pas apporter les correctifs qui empêcheront l'erreur de se reproduire, a-t-elle noté.

La commissaire a recommandé que l'ASSSSY prenne immédiatement des mesures pour élaborer et mettre en œuvre des politiques encadrant les communications avec les patients par des moyens non conventionnels, y compris le courriel, la fonction de numérisation et d'envoi par courriel, l'envoi de messages textes et d'autres moyens électroniques, en gardant à l'esprit les risques additionnels pour la protection de la vie privée dont il pourrait être nécessaire de tenir compte.

Les recommandations quant aux changements à apporter ont été acceptées, mais les délais proposés pour leur mise en place ne l'ont pas été. Aucun échéancier n'a été fourni.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION No 13-116

Le plaignant était persuadé que des renseignements tirés de son dossier d'adoption avaient été utilisés ou communiqués de manière inappropriée. Il a été adopté il y a plus de 40 ans dans une petite localité du territoire qui est aujourd'hui le Nunavut. Il alléguait que, quelque part entre 1997 et 2000, sa sœur adoptive

l'avait contacté en lui disant avoir deux numéros de téléphone pour lui : celui d'un préposé à l'adoption de Yellowknife et celui de sa mère naturelle, qui essayait de le retrouver et de reprendre contact avec lui. L'homme n'avait jamais souhaité connaître sa mère naturelle, mais il avait noté le numéro de téléphone de sa mère et avait finalement décidé de l'utiliser. Son expérience de reprise de contact n'a pas été positive.

En 2012, le plaignant a communiqué avec le ministère de la Santé et des Services sociaux pour obtenir une copie de son dossier d'adoption afin de savoir comment et pourquoi sa sœur adoptive avait eu accès à ses renseignements personnels. On lui a répondu qu'il devait remplir un formulaire, dans lequel étaient demandés de nombreux autres renseignements personnels. Ce formulaire aide le ministère à retrouver des membres de familles adoptives quand il reçoit des demandes en ce sens. Le plaignant a refusé de le remplir parce que son but n'était pas de reprendre contact avec sa famille, mais de découvrir comment des renseignements tirés de son dossier d'adoption s'étaient retrouvés entre les mains de sa sœur adoptive.

Les représentants du ministère ont indiqué que la mère naturelle du plaignant avait communiqué avec eux en vue de reprendre contact avec son fils. La *Loi sur l'adoption* confère au directeur des adoptions le droit de mener une enquête discrète quand un adopté ou l'un ou l'autre de ses parents naturels souhaite une reprise de contact. Dans ce cas, pour retrouver le plaignant, le directeur a contacté sa sœur, en la priant de demander à son

frère de communiquer avec le ministère. Selon le ministère, rien dans le dossier ne laisse penser que des renseignements concernant la mère biologique ou le plaignant ont été communiqués à la sœur de ce dernier.

Après avoir examiné le dossier d'adoption en question, la commissaire a confirmé que celui-ci ne contenait rien qui permette de penser que la sœur du plaignant avait obtenu quelque renseignement que ce soit au sujet de ce dernier ou de sa mère, sinon que le ministère tentait de retrouver le plaignant et que la mère de celui-ci souhaitait prendre contact avec lui. Le dossier contient toutefois très peu de détails permettant de déterminer avec exactitude ce qui s'est produit. Le dossier prouve que le plaignant a contacté le directeur et s'est vu transmettre les coordonnées de sa mère. Il montre aussi clairement que le plaignant a fini par décider de contacter sa mère naturelle.

La commissaire a commenté la manière dont le directeur des adoptions a traité la demande de renseignements du plaignant, c'est-à-dire comme une demande d'accès à son dossier d'adoption en vertu de la *Loi sur l'adoption*, plutôt que comme une demande en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*. Le plaignant ne demandait pas des informations lui permettant de prendre contact avec sa famille biologique, mais des informations sur la manière dont ses renseignements personnels avaient été utilisés ou divulgués.

La commissaire a recommandé, en ce qui a trait à la divulgation de renseignements provenant du registre des adoptions :

a) que toutes les conversations avec des familles naturelles souhaitant prendre part à des retrouvailles soient enregistrées, et que des notes indiquent clairement qui a contacté le ministère, quelle était la nature de la conversation et quelles mesures de suivi ont été convenues;

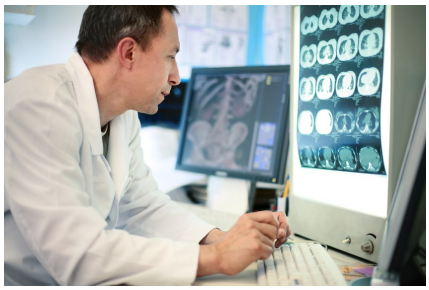
b) qu'avant que des renseignements sur la famille naturelle ne soient communiqués à un autre membre de la famille, un consentement à la divulgation soit obtenu par écrit et placé dans le dossier;

c) que lorsqu'ils recherchent des personnes liées par le sang, les employés divulguent le moins d'informations possible à des tiers quant aux raisons pour lesquelles ils recherchent une ou des personnes.

En ce qui concerne la demande du plaignant de voir tous les documents se rapportant à la manière dont lui et sa mère naturelle ont pu être remis en contact, la commissaire a recommandé qu'elle soit traitée comme une demande d'accès à l'information et que le plaignant obtienne tous les documents pertinents.

Les recommandations ont été acceptées.

REGARD VERS L'AVENIR



Le fait que j'aie reçu un si grand nombre de plaintes liées à la protection des renseignements médicaux personnels montre bien la nécessité de légiférer sur cette question. Je suis donc ravie de savoir que le gouvernement des TNO s'affaire à réglementer de manière plus spécifique l'accès à l'information et la protection de la vie privée dans le secteur de la santé; un projet de loi sera d'ailleurs bientôt présenté. Cela dit, cette nouvelle législation devra s'accompagner d'une importante campagne de sensibilisation s'adressant non seulement aux personnes qui travaillent dans le secteur de la santé, mais aussi à l'ensemble de la population. D'autres provinces et territoires au Canada ont déjà instauré une législation semblable et ont constaté qu'il leur a fallu du temps et des ressources avant son entrée en vigueur afin de s'assurer que chacun a toute l'information nécessaire pour bien comprendre les différentes dispositions et s'y préparer adéquatement. Il faudra aussi élaborer et mettre en œuvre de nouvelles politiques et procédures à l'intention des dépositaires des renseignements médicaux. Il y aura beaucoup de travail à faire pour veiller à ce que les citoyens aient une bonne compréhension pratique de la manière dont leurs renseignements médicaux personnels seront recueillis, utilisés et divulgués en vertu

de la loi. La nouvelle législation ne constituera néanmoins qu'une partie de l'équation. Les ressources nécessaires devront être consacrées à la fonction de surveillance qui est assurée par le Commissariat à l'information et à la protection de la vie privée. Cette nouvelle législation entraînera inévitablement une hausse de la charge de travail au sein du Commissariat, et je prévois qu'il faudra, plus tôt que tard, y augmenter le nombre de ressources humaines. Je le répète depuis plusieurs années, mais pour que je puisse faire le meilleur travail possible en qualité de commissaire à l'information et à la protection de la vie privée, il est de plus en plus nécessaire que j'y consacre de plus en plus de temps. Avec l'adoption de la nouvelle loi sur les renseignements médicaux, j'estime que la charge de travail connaîtra une croissance exponentielle et qu'il sera opportun d'envisager l'embauche d'un employé à temps plein qui pourra apporter son soutien dans le cadre des processus d'enquête, de médiation et de résolution de conflits.

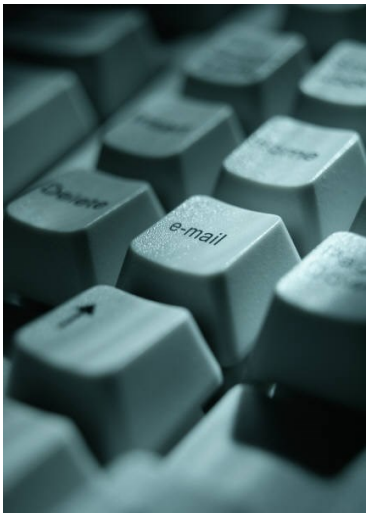
Par ailleurs, j'aimerais encore une fois encourager le gouvernement des TNO à trouver des façons d'inclure les municipalités dans le cadre de la *Loi sur l'accès à l'information et la protection de la vie privée* ou au moyen de leur propre législation. Il s'agit d'une recommandation que je formule depuis bon nombre d'années. Les commentaires que j'ai reçus à ce sujet ont généralement porté sur les coûts supplémentaires qui seraient encourus par les municipalités pour se conformer aux dispositions de la Loi. À mon avis, ces coûts sont nécessaires pour favoriser la transparence, la reddition de comptes et la démocratie. Cela dit,

si les coûts représentent la principale entrave, une solution à court terme – et relativement moins coûteuse – serait d'assujettir les municipalités à la Partie II de la Loi, soit celle qui a trait à la collecte, à l'usage et à la divulgation des renseignements personnels.

À la lumière du problème soulevé par la demande de révision no 12-108, j'estime qu'il serait également temps de commencer à discuter du fait que les gouvernements autochtones présents aux TNO doivent eux aussi veiller à assurer un accès à l'information conformément aux dispositions de la Loi et aux 10 principes de protection de la vie privée. Je comprends parfaitement que ce n'est pas là une chose qui est du ressort du gouvernement des TNO, mais j'encourage néanmoins tous les ordres de gouvernement à entamer la discussion.

Enfin, comme je l'ai mentionné brièvement dans mon message d'introduction, il est temps de revoir la Loi pour s'assurer qu'elle pourra effectivement tenir compte des changements dans les pratiques gouvernementales (p. ex. partenariats publics-privés, externalisation ou modèles de services partagés), sur le plan technologique, ainsi que dans les attentes des Canadiens à l'égard de la reddition de comptes des organismes publics. Les activités récentes de certains dénonciateurs activistes, comme Julian Assange et Edward Snowden, montrent que la population tend désormais à demander une plus grande transparence et une responsabilisation accrue de la part des gouvernements à l'égard du travail qu'ils effectuent. L'information est l'une des plus

importantes ressources naturelles de notre époque. Il s'agit non seulement d'une ressource précieuse, mais aussi d'une ressource publique. Les lois encadrant l'accès à l'information et la protection de la vie privée se doivent de tenir compte de la valeur croissante de cette ressource. Lors de leur assemblée annuelle de 2012, les commissaires à l'information et à la protection de la vie privée du Canada ont reconnu que la plupart des lois concernant l'accès à l'information et la protection de la vie privée qui sont actuellement en vigueur au pays ont relativement peu changé depuis les années 1980, et ils ont sommé toutes les administrations fédérales, provinciales et territoriales à moderniser et renforcer ces lois. À mon tour, je m'adresse au gouvernement des TNO pour qu'il procède à un examen approfondi de la Loi dans l'objectif d'y apporter des modifications qui permettront entre autres :



- de tenir compte de l'utilisation des technologies actuelles;
- d'exiger que tous les organismes du secteur public documentent adéquatement leurs délibérations, leurs actions et leurs décisions;
- d'établir des délais stricts et obligatoires pour les réponses aux demandes d'accès à l'information;
- de définir des normes minimales de divulgation proactive;
- de définir les exigences légales de notification aux individus affectés par la perte, le vol, ou l'utilisation ou la divulgation abusives de leurs renseignements personnels;

- d'établir une exigence pour les organismes du secteur public de prendre en compte le principe du respect de la vie privée dès la conception d'une nouvelle loi, d'un nouveau service, d'un nouveau programme ou d'une nouvelle politique (p. ex. en exigeant une évaluation des répercussions sur la vie privée ou en instaurant une protection intégrée de la vie privée).

ANNEXE A

Modernisation des lois sur l'accès à l'information et la protection des renseignements personnels au XXIe siècle

CONTEXTE

La population canadienne s'attend désormais à une plus grande responsabilisation et transparence de la part des gouvernements et des entreprises privées relativement à la façon dont ils recueillent, créent, partagent, divulguent et gèrent l'information, y compris les renseignements personnels.

Au fil des ans, il y a eu de nombreux changements technologiques, de même que des modifications aux pratiques gouvernementales (par ex. partenariats publics-privés, sous-traitance ou modèles de services partagés) et aux attentes des Canadiens. Les Canadiens sont de plus en plus inquiets de l'érosion de leurs droits à la vie privée à la lumière des révélations récentes sur les programmes de surveillance gouvernementaux. Ces révélations ont également engendré un plaidoyer en faveur d'une plus grande transparence et une surveillance plus rigoureuse des initiatives relatives à la sécurité nationale.

Depuis leur adoption il y a plus de vingt ans, la plupart des lois canadiennes sur l'accès à l'information et la protection des renseignements personnels n'ont pas réellement été modifiées de manière à s'adapter à ces changements ou à améliorer les protections et les droits qu'elles accordent. Seules quelques lois canadiennes ont récemment été adoptées ou modifiées pour faire face aux défis modernes et assurer la protection continue des droits de chacun à l'accès à l'information et à la protection des renseignements personnels.

Durant cette période, le législateur a également modifié ou adopté des lois ayant eu pour effet de fragiliser ou d'éroder les droits relatifs à l'accès à l'information et à la protection des

renseignements personnels – droits que les lois sur l'accès à l'information et la protection des renseignements personnels visaient à protéger et à garantir.

Ailleurs dans le monde, les lois sur l'accès à l'information et la protection des renseignements personnels ont été renforcées pour s'adapter aux réalités du XXIe siècle, telles que l'évolution des technologies de l'information et de la communication, le défi que représente la gestion de l'information électronique, ainsi que les demandes sociales et politiques des citoyens engagés. Les lois canadiennes doivent suivre cette tendance.

ATTENDU QUE

L'information est l'une des ressources nationales les plus importantes du Canada.

L'accès à l'information et la protection des renseignements personnels sont des valeurs fondamentales pour les Canadiens. Ils font partie de nos droits et libertés démocratiques.

Les Canadiens doivent pouvoir se fier aux institutions publiques et aux entreprises privées, qui sont responsables des pratiques relatives à la protection des renseignements personnels, des décisions qu'elles prennent en matière d'accès et de leurs méthodes de gestion de l'information.

Le Canada doit regagner sa position de chef de file dans les domaines de l'accès à l'information et de la protection des renseignements personnels.

EN CONSÉQUENCE

1) Les commissaires et les ombudsmans à l'information et à la protection de la vie privée au Canada font appel à leurs gouvernements respectifs pour réitérer leur engagement envers les valeurs démocratiques qui sont à la base de l'accès à l'information et de la protection des renseignements personnels en :

- consultant le grand public, la société civile et les commissaires et les ombudsmans à l'information et à la protection de la vie privée sur la meilleure façon de moderniser les lois sur l'accès à l'information et la protection des renseignements personnels à la lumière des

technologies de l'information modernes, des pratiques gouvernementales en évolution et des attentes des citoyens;

- modernisant et renforçant ces lois en se basant sur la législation plus actuelle et progressiste en vigueur dans certaines régions du Canada et dans le reste du monde, y compris tous ou certains des éléments suivants :

Pour l'accès à l'information :

a) Accorder de véritables pouvoirs d'application et de surveillance de la loi permettant notamment d'émettre des ordonnances de divulgation et d'imposer des pénalités en cas de non-respect de celles-ci;

b) Préciser quels organismes du secteur public sont visés par les lois sur l'accès à l'information et en élargir la portée;

c) Exiger que tous les organismes du secteur public documentent leurs délibérations, leurs actions et leurs décisions;

d) Établir des délais stricts et de rigueur afin que les organismes du secteur public répondent aux demandes d'accès à l'information de façon diligente;

e) Lorsque les restrictions se fondent sur un risque de préjudice pouvant résulter de la divulgation, obliger les organismes publics à démontrer que ce préjudice est réel et important de manière à limiter le nombre de documents qui sont exemptés du droit général d'accès à l'information;

f) Exiger qu'un document soit divulgué, y compris un document visé par des restrictions au droit d'accès, lorsqu'il est manifestement nécessaire d'agir ainsi dans l'intérêt public;

g) Définir des normes minimales de divulgation proactive, y compris l'établissement de classes ou de catégories de dossiers que les entités du secteur public doivent

mettre à la disposition du public de façon proactive et, en accord avec les objectifs des données ouvertes, les rendre disponibles dans un format utilisable;

h) Exiger que la nécessité de toute exception et exclusion à l'accès à inclure dans des lois autres que celles relatives à l'accès à l'information soit démontrée et que les gouvernements consultent les commissaires et les ombudsmans à l'information et à la protection de la vie privée;

i) Établir une exigence pour les organismes du secteur public de prendre en compte l'accès à l'information lorsqu'ils créent de nouveaux systèmes, en s'assurant par le fait même que l'exportation des données soit possible et facile.

Pour la protection des renseignements personnels :

a) Renforcer les pouvoirs d'application et de surveillance de la loi et les pénalités prévues en cas de contravention à celle-ci;

b) Préciser quels organismes du secteur public sont visés par les lois sur la protection de la vie privée et en élargir la portée;

c) Définir les exigences légales de notification aux individus affectés par la perte, le vol, la destruction, ou l'utilisation ou la divulgation abusives de leurs renseignements personnels (notification obligatoire des atteintes à la protection des données);

d) Exiger que les organismes du secteur public améliorent l'information qu'ils fournissent au sujet de leurs politiques et pratiques en matière de protection des renseignements personnels;

e) Établir un « test de nécessité » en vertu duquel les organismes du secteur public et privé doivent prouver qu'ils ont besoin d'obtenir les renseignements personnels qu'ils recueillent;

f) Prévoir des moyens efficaces permettant aux individus de faire valoir leurs droits relatifs à la protection des renseignements personnels et de se plaindre ou de dénoncer le non-respect, par un organisme public, de ses obligations législatives;

g) Renforcer les exigences de déclaration au public relatives à la divulgation des renseignements personnels entre les entreprises privées les organismes du secteur public;

h) Exiger des organismes du secteur public et privé qu'ils mettent en œuvre des programmes de gestion des renseignements personnels afin d'en assurer leur protection;

i) Établir une exigence pour les organismes du secteur public de prendre en compte le principe du respect de la vie privée dès la conception d'une nouvelle loi, service, programme ou politique (par exemple, l'évaluation des facteurs relatifs à la vie privée, protection intégrée de la vie privée).

2) Les commissaires et les ombudsmans à l'information et à la protection de la vie privée au Canada s'engagent à :

- collaborer avec leur gouvernement, la législature et le Parlement sur les enjeux décrits ci-dessus et à en assurer le suivi;
- continuer d'étudier comment les lois sur l'accès à l'information et sur la protection des renseignements personnels affectent tous les Canadiens et de rendre cette information publique;
- formuler des recommandations destinées à leur gouvernement, à la législature et au Parlement selon leur domaine d'expertise.

Liste des signataires

Jennifer Stoddart, Commissaire à la protection de la vie privée du Canada

Suzanne Legault, Commissaire à l'information du Canada

Elizabeth Denham, Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique

Jill Clayton, Commissaire à l'information et à la protection de la vie privée de l'Alberta

Mel Holley, Ombudsman du Manitoba par intérim

Anne E. Bertrand, Commissaire à l'accès à l'information et à la protection de la vie privée du Nouveau-Brunswick

Ed Ring, Commissaire à l'information et à la protection de la vie privée de Terre-Neuve-et-Labrador

Elaine Keenan Bengts, Commissaire à l'information et à la protection de la vie privée des Territoires du Nord-Ouest et commissaire à l'information et à la protection de la vie privée du Nunavut

Dulcie McCallum, Agente de révision (commissaire), Bureau d'examen de l'accès à l'information et de la protection de la vie privée de la Nouvelle-Écosse

Ann Cavoukian, Commissaire à l'information et à la protection de la vie privée de l'Ontario

Maria C. MacDonald, Commissaire à l'information et à la protection de la vie privée de l'Île-du-Prince-édouard

Maître Jean Chartier, Président, Commission d'accès à l'information du Québec

R. Gary Dickson, Commissaire à l'information et à la protection de la vie privée de la Saskatchewan

Diane McLeod-McKay, Ombudsman et commissaire à l'information et à la protection de la vie privée du Yukon