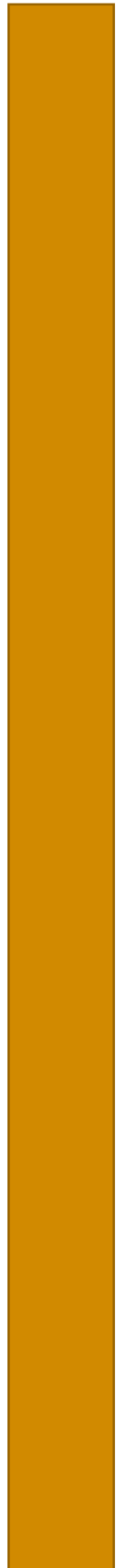




OFFICE OF THE INFORMATION AND
PRIVACY COMMISSIONER OF NUNAVUT

ANNUAL REPORT

2018-2019





OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER

JE H. HAZZEL

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

July 10, 2019

Legislative Assembly of Nunavut
P.O. Bag 1200
Iqaluit, NU
X0A 0H0

Attention: Simeon Mikkungwak
Speaker of the Legislative Assembly

Dear Sir:

I have the honour to submit to the Legislative Assembly my Annual Report as the Information and Privacy Commissioner of Nunavut for the period of April 1st, 2018 to March 31st, 2019.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

Contents

COMMISSIONER’S MESSAGE	3
ACCESS TO INFORMATION AND PROTECTION OF PRIVACY IN BRIEF	7
Access to Information	7
Protection of Privacy.....	8
The Role of the Information and Privacy Commissioner	9
THE YEAR IN REVIEW	11
REVIEW REPORTS	14
Review Report 18-143.....	14
Review Report 18-144.....	15
Review Report 18-145.....	16
Review Report 18-146.....	17
Review Report 18-147.....	18
Review Report 18-148.....	19
TRENDS AND ISSUES – MOVING FORWARD	21
Legislation	21
Policies.....	23
Cannabis and Privacy.....	23
Leadership and Adequate Resources.....	24



COMMISSIONER'S MESSAGE

I am pleased to present our 2018-2019 annual report. If there were a theme to this year's Annual Report, it would be "change". The world, and the way in which we all interact with it, is changing day by day, though the rights protected by Nunavut's access and privacy legislation remain as relevant and important as they were when the legislation was written more than 20 years ago. In fact, those rights are exponentially more important today than they were 20 years ago. Nunavut's *Access to Information and Protection of Privacy Act* was written in the mid 1990's. There have been amendments from time to time to address discrete issues, but there has been no overall review of the Act to ensure that it is adequate to meet the demands of today's digital government and economy. When the *Access to Information and Protection of Privacy Act* was written, there was an awareness that there was a "thing" called the internet and that it held promise as a tool for communication, but it was not widely used or understood by the general public. We were still a paper-based society. As incredulous as it might sound to today's generation, there was no immediate way to verify facts. If you wanted to look something up, you took a trip to the library and looked things up in the Encyclopaedia. The concept of "keywords" was unknown. There was no "Siri" and no "Google". It took time and effort to obtain information. It was also much easier to maintain your privacy, because paper was difficult and time consuming to track. There was no artificial intelligence and computers were much too large to carry with you from place to place. The mobile phones and devices that we all carry around in our pockets today contain technology that is infinitely more powerful and sophisticated than the technology used to send men to the moon in the first several Apollo missions.

Quite simply, we live in a different world. Today, the public expects and demands instant gratification when it comes to obtaining answers to questions. The public demands and expects governments to share more information about the way they do business in a much more revealing way than was expected 20 years ago. Lack of transparency today has far more instantaneous and significant consequences than was historically the case. Furthermore, personal information - information about individuals and how we each live, work, and play - is now a valuable commodity which is regularly collected, used, bought, sold and manipulated. Vast amounts of information about each of us is collected and saved every day. Governments are some of the most prolific collectors of personal information and in circumstances which often do not afford the public a choice as to whether or not to participate.

It is time to take a good long look at the law which governs how that information is collected, used, disclosed, stored, and managed. It is time that we modernize our access and privacy legislation to take these changes into account. Nunavut took some early steps toward modernization when it was the first jurisdiction in the country to include a requirement for all public bodies to report breaches of privacy, but a much more wholistic approach is needed. Nunavut still does not have health privacy legislation and is the only jurisdiction in Canada, with the exception of British Columbia, where this is the case. That said, while British Columbia does not have stand alone health privacy legislation, there are a number of pieces of legislation in that jurisdiction which address the unique privacy concerns surrounding health data in the province.


The fate of access and privacy rights in Nunavut depends on us keeping pace with technology and ensuring that our rights are subject to meaningful and effective oversight. This will require leadership, focus and intention – not only to undertake a complete review of the legislation and make changes to bring Nunavut into the twenty-first century, but also to ensure that the legislation is respected and compliance encouraged. There has been a not-so-subtle shift in the government's approach to

dealing with its obligations under the Act. In recent years the “corporate culture” within many public bodies has shifted such that instead of public bodies making genuine and concerted effort to assist applicants and to comply with the general purposes and intentions of the Act, they appear to be trying to find ways to avoid or over-ride those purposes and intentions. Leadership is key in this and, as noted in last year’s Annual Report, leadership in this regard has been waning over time. This needs to change.

Speaking of change, I would like to formally welcome and introduce our Assistant Information and Privacy Commissioner, Dylan Gray, who joined the office in March of 2019. Dylan comes to us from the Northwest Territories Department of Health, where he was a Privacy Specialist. He brings a wealth of information and enthusiasm to the office and his arrival has made my job much easier. The volume of work has been increasing steadily and exponentially over the last few years and his presence will help to recover some ground from the backlog that has developed.

Again, on the topic of change, in 2020 I will be retiring and, for the first time since Nunavut was created, there will be a new Information and Privacy Commissioner. While I expect that I will be preparing one last Annual Report for next year, I do want to take this opportunity to recognize all those who have been access and privacy champions in Nunavut and who have helped me to spread the message. ATIPP Coordinators in public bodies do not have the most glamorous jobs, nor is the work conducive to getting pats on the back. It is a difficult and sometimes unpopular job. It has, however, been my pleasure to work with each of them. I would, however, like to give special acknowledgment to Jessica Young, who held the position of Manager of ATIPP for the GN for the last number of years and who, in that position, was the number one champion for access and privacy rights. Jessica recently moved out of the position and on to new ventures. I look forward to working with the new Manager of ATIPP, Mark Witzaney.

Finally, and perhaps most importantly, I would like to thank my assistant, Lee Phypers, who manages to get everything done with a smile and good humour, no matter what's going on in the office.



CITIZENS AND GOVERNMENTS HAVE BECOME INCREASINGLY AWARE OF THE NEED TO MODERNIZE ACCESS AND PRIVACY LAWS TO ENSURE THAT THEY CONTINUE TO ENSHRINE MEANINGFUL AND ENFORCEABLE RIGHTS. MOST IMPORTANTLY, THE LAWS NEED TO ADAPT SO THAT THEY CAN CONTINUE TO SERVE THEIR ORIGINAL PURPOSES OF THESE LAWS THAT REMAIN RELEVANT TODAY.

Accountability for The Digital Age
Modernizing Nova Scotia's Access and Privacy Laws
A Report by The Information and Privacy
Commissioner for Nova Scotia (June, 2017)

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY IN BRIEF

The *Access to Information and Protection of Privacy Act* (ATIPPA) confirms two fundamental rights:

1. the **right** of the public to have access to public records; and
2. the **right** of the public to have the personal information that the Government of Nunavut collects about them individually to be protected from unauthorized use or disclosure.

The Act outlines the rules by which the public can obtain access to public records and establishes rules about the collection, use and disclosure of personal information collected and maintained by Nunavut public bodies. It applies to 43 departments, crown corporations, local housing organizations and other agencies in Nunavut.

Access to Information



Part I of the legislation gives the public the right to request and receive public records and a process for obtaining such records. This right of access is so important to the maintenance of open and accountable government that access to information laws have been deemed to be quasi-constitutional in nature. When the public can see how government is functioning and how they are doing their work, they are better able to participate in government and to hold government and governmental agencies to account. The right of access to government records is not, however, absolute. There must be some exceptions and these limited and specific exceptions are set out in the legislation. Most of the exceptions function to protect individual privacy rights and proprietary business information of the companies which do business with the Government of Nunavut. The

exceptions also function so as to allow Ministers and their staff to have free and open discussions as they develop policies and deal with issues.

Requests for Information must be in writing and delivered to the public body from which the information is sought. When a Request for Information is received, the public body must first identify all of the records which respond to the request, then assess each record and determine what portion of that record should be disclosed and what might be subject to either a discretionary or a mandatory exception. This is a balancing act which is sometimes difficult to achieve. The response must be provided to the Applicant within 25 business days.

If an Applicant is not satisfied with the response provided by the public body, an request can be made to the Information and Privacy Commissioner to review the response given.

Protection of Privacy



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

This part of the Act also gives individuals the right to ask that the public body correct personal information that is in error.

Part II of the Act also requires public bodies which know or have reason to believe that there has been a material breach of privacy with respect to personal information under its control to report that breach of privacy to the individual whose information has been wrongfully disclosed and to the Information and Privacy Commissioner.

The Role of the Information and Privacy Commissioner



The Office of the Information and Privacy Commissioner (OIPC) was established under the Access to Information and Protection of Privacy Act of the Northwest Territories in 1997, prior to division. This legislation was continued in Nunavut on Division Day in 1999. The Information and Privacy Commissioner (IPC) is appointed by the Commissioner of Nunavut on the recommendation of the Legislative Assembly and holds that appointment for a five-year renewable term. This role is currently held by Elaine Keenan Bengts, whose term expires in May, 2020.

The role of the Information and Privacy Commissioner (IPC) is to provide independent oversight over public bodies as they apply the Access to Information and Protection of Privacy Act. The independence of the role is vital to the work of the IPC as it allows her to openly criticize government, when necessary, without fear of being removed from office.

When someone has asked for information from a public body and is not satisfied with the response received, they may request a review by the Information and Privacy Commissioner. The IPC is able to see all responsive records and, based on the input of both the Applicant and the public body, will prepare a report and make recommendations. The Information and Privacy Commissioner does not have any power to compel public bodies to either disclose or protect information from disclosure but she is required to provide the Minister of a department or the CEO of a public

corporation with recommendations. The Minister or CEO must decide to either accept the recommendations made or to take such other steps as they deem appropriate, within 30 days. The Applicant has the right to appeal the Minister's or CEO's decision to the Nunavut Court of Justice if there continues to be a dispute as to the proper application of the Act to the records in question.

The Information and Privacy Commissioner is also authorized to investigate privacy complaints, including complaints about the failure or refusal of a public body to make a correction to an individual's personal information. Any person may file a complaint about a privacy issue with the Information and Privacy Commissioner. The IPC will investigate and prepare a report and make recommendations for the Minister or CEO.

The Information and Privacy Commissioner is also authorized to initiate an investigation of a privacy issue of her own accord when information comes to her attention which suggests that a breach of privacy may have occurred.

As in the case of an Access to Information review, the Minister or CEO of the public agency involved must respond to the recommendations made by the Information and Privacy Commissioner in privacy breach matters. In these cases, however, the Minister or CEO has 90 days to respond, and there is no right of appeal from the decision made.





THE YEAR IN REVIEW

The Office of the Information and Privacy Commissioner opened thirty-four (34) files in the 2018 – 2019 fiscal year which is about the same number of files opened in the previous year (35).

During fiscal 2018/19, files opened by the OIPC included consideration of several categories of issues:

Access to Information Matters

General Requests for Review	8
Extension of Time	1

Breach of Privacy Matters

Privacy Breach Notifications	10
Privacy Breach Complaints	5
IPC Initiated Matters	3

Request for Comments/Consultations 5

Administrative 1

Miscellaneous (Smart Cities Challenge) 1

This represents a significant increase of breach notifications from public bodies pursuant to section 49.9 of the Act. That said, the number of privacy breach notifications should be much, much higher. Section 49.9 of the Act requires public bodies to report “material” breaches of privacy to the Information and Privacy Commissioner. When

those material breaches pose a real risk of significant harm to the individual, the individual must also be told. In each of my last two Annual Reports, I have commented on the fact that, despite section 49.9, the number of Breach Notifications received by my office is still very low. In today's information age, there are good reasons for requiring governments (and businesses) to be hyper vigilant and transparent when mistakes are made that result in a breach of the privacy of individuals. When the public is not aware that their personal information has been collected, used or disclosed in an inappropriate way, they are unable to defend themselves from misuse of that information. Lack of transparency with respect to privacy breaches will also result in the erosion of trust in government. The public often does not have any choice but to provide significant personal information to government – health, education, social benefits, taxation, worker's compensation by way of example - all require individuals to give up sensitive personal information to receive services. This information, if inappropriately used or disclosed can cause financial, social, emotional and even physical harm. It is incumbent on government, both legally and ethically, to be open, honest and transparent when a breach occurs. The obligation to report breaches must become the immediate and automatic response. Reporting breaches not only gives individuals the ability to take mitigation measures, but also helps to identify the gaps in policies and procedures that are causing such breaches. Transparency allows analysis of these events and the identification of trends. This, in turn leads to the identification of causes and solutions that can be implemented to resolve breaches before they happen. Understanding the weaknesses in policies and procedures allows for the identification of means and ways to address those weaknesses proactively, so they don't continue to weigh down and distract from the important work of providing services to the public, while giving the public confidence that they can share their personal information and personal health information with public servants safely. Privacy is important. It is foundational to the ability of the public service to serve citizens.

Privacy breaches happen every day. Misdirected faxes, lost mobile devices (including jump drives, laptops, tablet and cell phones), gossiping, snooping, excessive collection of information --- all of these things happen every day. Almost any breach involving personal health information or financial information or social information would amount to a “material” breach under the Act. Public bodies are either not recognizing breaches when they occur or, in the alternative, they are purposely ignoring their responsibility under the Act to report those instances. It makes no sense to have cutting edge provisions in the legislation if those provisions are ignored. This has to improve.



The Information and Privacy Commissioner
Appearing before Standing Committee on
Oversight of Government Operations and
Public Accounts – April 11, 2019

REVIEW REPORTS

Six Review Reports were issued by the Office of the Information and Privacy Commissioner in fiscal 2018/2019.

Review Report 18-143

Category of Review: Privacy Breach (Commissioner Initiated Review)
Public Body Involved: Department of Health
Sections Applied: Section 49.2, Section 49.7, Section 49.8, Section 49.9
Section 49.10
Outcome: Recommendation not accepted

This matter came to the attention of the Information and Privacy Commissioner as a result of a news report about an individual concerned about how the Department of Health was handling medical records. He had reported that when attending a clinic to get medical treatment, medical personnel found his wife's information in his chart. When he asked the practitioner about whether the incident would be reported, he had allegedly been told simply that "it happened all the time" and that there was really nothing to report. The Department acknowledged the incident and indicated that it had, in fact, been reported to the Supervisor of Community Health Programs. The page had been removed from the individual's file and returned to the proper chart. The patient had not seen what was on the page.

The Information and Privacy Commissioner (IPC) found that the misfiling of the page constituted a "loss" of the record and, therefore, a breach of the wife's privacy. She also found that the breach was "material" because it pointed to systemic issues and involved the wife's personal health information. The breach, therefore, should have been reported to the Information and Privacy Commissioner. The nature of the record and the breach were, however, not such as to raise a reasonable expectation of harm for the wife and there was, therefore, no obligation on the department to give her notice.

The Department had advised the CBC reporter who had written the story that the onus was on the patient to report a breach of privacy. The Information and Privacy Commissioner made it clear that this was not the case and that section 49.1 requires public bodies to report material breaches of privacy to the IPC.

The Information and Privacy Commissioner recommended that all employees of health clinics and facilities in Nunavut be provided with formal training with respect to their obligations under the *Access to Information and Protection of Privacy Act*. The Department's response only committed to following up with health centres and staff on the procedure for addressing misfiled records.

Review Report 18-144

Category of Review: Access to Information
Public Body Involved: Department of Community and Government Services
Sections Applied: Section 1, Section 5, Section 24(1), Section 28
Outcome: Recommendations accepted

A request was received by the Department of Community and Government Services (CGS) for access to all proposals submitted in response to the RFP for the delivery of a law degree program in Nunavut. One of the proponents objected to the proposed disclosure after a third-party consultation as required by section 28 of the Act. They argued that the disclosure was contrary to section 24 in that the proposal contained confidential business information.

The Information and Privacy Commissioner found that while some of the information in the proposals was proprietary information owned by the proponents and provided to the Department in confidence, there were large sections of the proposal which could be disclosed because the information in these sections was publicly advertised by the proponent on their own web site and in other publications. Those parts of the proposal,

therefore, could not be said to have been provided to the Department “in confidence” and did not meet the criteria for an exemption under section 24. She recommended the disclosure of large parts of the proposals.

Review Report 18-145

Category of Review: Access to Information
Public Body Involved: Department of Justice
Sections Applied: Section 14(1)(a), Section 15(a), Section 16(1)(a), Section 16(1)(c), Section 20(1)(c), Section 20.1, Section 23
Outcome: Recommendations accepted with the exception of recommendations under section 20.1

The Applicant sought information in relation to a Coroner’s Inquest in relation to a specific incident. The Department significantly redacted the responsive records relying on several sections of the Act, in particular section 20.1 which prohibits the disclosure of information “relating to an active coroner’s investigation or inquest”.

The Information and Privacy Commissioner found that section 20.1 did not apply to correspondence between officials which did not reveal anything about the active coroner’s investigation or inquest. Most of the correspondence to which section 20.1 was applied were not about the active investigation but about process generally and, while discussed tangentially in the context of a particular investigation, did not reveal anything about the evidence gathered in or related to the investigation itself.

Each of the redacted items in the response was reviewed and recommendations were made as to disclosure under the other sections of the Act relied upon.

Review Report 18-146

Category of Review:	Access to Information
Public Body Involved:	Department of Justice
Sections Applied:	Section 14(1)(b), Section 15(c), Section 16(1)(a), Section 16(1)(c), Section 20(1)(c), Section 20(1)(f) and Section 23(1)
Outcome:	Accepted in part

The Applicant requested information in relation to the policies and procedures of the Coroner's Office in relation to the investigation of police-involved shootings in Nunavut. Most of the responsive records provided to the Applicant in response to his request were significantly redacted. The public body originally relied on sections 14, 15, 16, 20 and 23 of the Act. After the request had been made, but before the response was provided, amendments were made to the *Access to Information and Protection of Privacy Act* and the public body sought, retroactively, to rely on a new section – Section 20.1 which prohibits the disclosure of information relating to an active coroner's investigation or inquest.

The IPC found that the information which the public body sought to withhold was not "information relating to an active coroner's investigation" but was rather information about the way in which police-involved shootings are generally handled in Nunavut. The Department of Justice disagreed with this assessment. However, by the time the recommendations were made and responded to, there was no longer an "active coroner's investigation" and they withdrew their reliance on that section of the Act, relying, once again, on the other cited sections. The IPC reviewed each of the redacted items and made recommendations, some of which were accepted and others not.

Review Report 18-147

Category of Review:	Access to Information – Extension of Time
Public Body Involved:	Department of Culture and Heritage
Sections Applied:	Section 1, Section 5, Section 7, Section 8, Section 11(1)(c), Section 26
Outcome:	Recommendations acknowledged, but not clearly accepted

The Applicant in this case had made an extremely extensive request for information. The request had been made in extremely broad terms and would have taken the Department many hundreds of hours to respond fully. The request was dated October 24th. On November 6th, the public body acknowledged receipt of the request. On November 29th, a letter was sent to the Applicant indicating that the public body was extending the time for their response by 120 days so that they could consult with others, indicating that the response would be provided by March 9th. The Applicant objected to the length of the extension.

The Information and Privacy Commissioner noted that:

- section 7 of the *Access to Information and Protection of Privacy Act* public bodies are charged with a positive “duty to assist” applicants and that this includes contacting Applicants directly to try to narrow and hone broadly worded applications such as the one in question but that there was no evidence that any effort had been made to do this
- in a case like this, where it is clear that there will be fees associated with the response, every effort should be made to contact the Applicant early in the process to discuss those fees but that there was no evidence that the issue of fees had even been raised until nearly six months after the Request for Information had been submitted and the matter was already before the Information and Privacy Commissioner to review the extension of time

- while the nature of this request would most likely have justified an extension of time pursuant to Section 11 of the Act, the subsection of section 11 used by the public body to justify the extension was the wrong subsection;
- an extension of over four months, even in the circumstances of this case, was not a “reasonable” extension of time;
- that the public body’s explanation with respect to the consultations necessary was not sufficient to justify the need for such consultations.

Recommendations were made to change processes and procedures. While those necessary changes were acknowledged by the Minister in his response, there was no commitment to make the necessary changes to ensure these errors would not happen again.


Review Report 18-148

Category of Review: Access to Information
Public Body Involved: Department of Health
Sections Applied: Section 1, Section 23
Outcome: Analysis accepted but Recommendations not accepted.

The request in this case was for statistical information on a community by community basis on the incidence of tuberculosis (TB) in Nunavut. The Department of Health disclosed some information, but declined to disclose community level numbers because of the risk of re-identification with small numbers.

The Information and Privacy Commissioner agreed with the Department that the risk of identifying individuals in communities diagnosed with TB was significant for those communities with small populations and only a few diagnosed cases. She held that there was no hard and fast rule for when the statistics might reveal more than merely statistics, but that each situation had to be evaluated on its own merits. She recommended the disclosure of some additional information, but not all of it.

While the Department of Health agreed with the analysis of the issues in the IPC's report, they decided to err on the side of caution and refused to disclose any additional information.



ENSURING THAT PERSONAL INFORMATION HELD BY AN ORGANIZATION IS ACCESSED ONLY BY EMPLOYEES WHO NEED IT, AND ONLY AT TIMES THAT INFORMATION IS REQUIRED FOR LEGITIMATE BUSINESS PURPOSES, CAN BE A CHALLENGE — BUT IT IS A CHALLENGE THAT NEEDS TO BE ADDRESSED. WITHOUT APPROPRIATE PREVENTATIVE SAFEGUARDS, HUMAN CURIOSITY AND OTHER MOTIVATIONS (INCLUDING SINISTER ONES, SUCH AS PROFIT AND/OR HARM TO INDIVIDUALS) CAN LEAD EMPLOYEES TO ACCESS PERSONAL INFORMATION WITHOUT AUTHORIZATION AND WITHOUT A LEGITIMATE BUSINESS PURPOSE — ALSO KNOWN AS “EMPLOYEE SNOOPING”

TEN TIPS FOR ADDRESSING EMPLOYEE SNOOPING, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, MARCH, 2016

TRENDS AND ISSUES – MOVING FORWARD

It is time. Time for change. Time for a full and comprehensive review of the existing legislation and time to create new legislation to deal with privacy in the health sector.



But legislative change isn't the be all and the end all. Legislation without leadership achieves little. So, it is also time to change the idea that access and privacy matters are secondary considerations that can be "worked around". It is time to ensure that the work of those tasked with the management of access and privacy matters in each public body are given the resources, the training and the power they need to make good decisions. It is time that, when evaluating job descriptions for positions that include a role in the administration of the *Access to Information and Protection of Privacy Act*, the importance and difficulty of the role is recognized and that compensation levels are assigned accordingly. It is time for all in senior management to recognize that the *Access to Information and Protection of Privacy Act* is a piece of legislation which plays a fundamental role in achieving a healthy democracy despite the closer scrutiny it invites. It is time that ministers, deputy ministers and senior managers take an active leadership role to promote adherence to the legislated duties imposed by the Act and to foster an atmosphere in which employees are encouraged to comply with the spirit and intention of the legislation. It is time that the expertise inherent in the role of the Information and Privacy Commissioner is acknowledged and that the Information and Privacy Commissioner is given the tools necessary to ensure that the work that she does receives something more than a passing nod.

Legislation

Nunavut is now the only jurisdiction in Canada that has not done a comprehensive review of their first-generation access and privacy legislation. It is the only jurisdiction in

Canada which has not recognized, through legislation, that the management of personal health information involves a significantly different approach than the management of other kinds of personal information. As in previous annual reports, I encourage the Government of Nunavut to undertake a comprehensive review of the *Access to Information and Protection of Privacy Act* with a view to including amendments to bring the legislation up to date with technology and to give the legislation more visibility and respect. Nunavut was the first jurisdiction in Canada to require that all public bodies to notify the Information and Privacy Commissioner of material breaches of privacy. That was a start, but was not enough. Other changes that should be considered are provisions with respect to pro-active disclosure, a “public interest” over-ride to the exceptions from disclosure to ensure that the public is informed when there are serious issues that might directly affect them, changes to the powers of the Information and Privacy Commissioner so that recommendations made by the office have real impact, a requirement for review of privacy impact assessments prepared in advance of new programs being considered or existing programs being changed, and the mandatory adoption of “privacy by design” for new projects.

I once again strongly suggest that the Department of Health develop health specific privacy legislation which recognizes the need for the sharing of personal health information to provide good health service to the public, while at the same time recognizing the rights of clients and patients to know, understand and retain control over how their personal health information is being used and disclosed. This is a long-standing recommendation. The ATIPP Act which currently applies to health information in the same way as it applies to personal information in general simply does not meet the needs of the health sector or give patients necessary control over their own personal health information. There needs to be far more direction and far more detail about what is acceptable collection, use and disclosure of personal health information so that health professionals do not find themselves inadvertently in breach of the *Access to Information and Protection of Privacy Act* on a daily basis.

Policies

I am once again strongly recommending a comprehensive review of policies and procedures in relation to the management of digital records. In my experience, the existing policies are hard to find, poorly written and clearly dated. In at least one instance, there is reference to legislation which does not even exist in Nunavut. There are no policies surrounding the use of personal devices or personal email accounts for conducting GN business, but it is clear that this is a common practice. There is nothing to direct when the use of personal devices/email addresses is acceptable. How are those records being retained for future reference? Are there any security requirements? Is it clear that the use of a personal device or the use of a personal email address for doing government business might result in a search of those devices or emails to respond to an ATIPP request? Is there an understanding or a requirement that when an employee leaves the GN he/she is to ensure that all government related records are appropriately transferred to the GN system and deleted from personal devices/emails? I have been unable to find any policies or statements in relation to any of these issues. Most of the work of GN employees in today's business environment is digital. While this makes the work easier and employees more efficient, it also places on public bodies the obligation to ensure that information is not being mishandled. Formal policies and procedures must keep up with the technology.

Cannabis and Privacy

With the legalization of cannabis all Canadian jurisdictions have been struggling with privacy issues in relation to the purchase of cannabis products. While now legal in Canada, cannabis is not legal in many other countries, including the United States and it is unclear how evidence of legal cannabis use might be used by other countries in restricting entry into the country or in dealing with an individual who has run into legal difficulties while travelling in another country. Furthermore, while legal, cannabis use is still subject to stereotyping and stigma. It is imperative that the personal information of

those purchasing legal cannabis is protected and that the necessary security is in place to prevent either intentional or inadvertent disclosure. Careful consideration must be given to the amount of information collected, the security around the on-line systems and retention and destruction of information collected when it is no longer necessary. A thorough and independent Privacy Impact Assessment must be done to ensure that all privacy issues are identified and addressed.

Leadership and Adequate Resources

As noted above, even the best legislation and the best policies and procedures will not make much of a difference if leadership is not evident. The *Access to Information and Protection of Privacy Act* places positive duties on public bodies. It provides for independent oversight in the form of an Information and Privacy Commissioner to ensure that public bodies comply with the Act. But the Information and Privacy Commissioner can only make recommendations. Many public bodies have learned over the years that there few, if any, consequences when time-lines imposed by the legislation are ignored, or when the processes set out in the Act are glossed over, or when they do not respond to correspondence from the Information and Privacy Commissioner or, for that matter when recommendations made by the Information and Privacy Commissioner are either glossed over, ignored or outright rejected. This is not a legislative issue. It is a leadership issue. ATIPP matters are routinely given low priority in relation to the other job responsibilities of ATIPP Coordinators. This is possible because leadership allows it, and in fact expects it – because leadership puts priority on other aspects of the Coordinator’s job. Human resources are limited and often insufficient to meet all of the needs of the department. Access to information requests in these circumstances are given low priority. There are few GN employees whose job it is to advocate with respect to privacy issues on a pro-active basis. Privacy concerns and privacy issues are simply not addressed except in a re-active way. The proliferation of “information sharing agreements” requires careful attention to privacy issues, but that

attention appears to be lacking. Training for new ATIPP Co-ordinators does not appear to be sufficient to impart the basic concepts, let alone the detailed knowledge to effectively and efficiently address complex access and privacy inquiries.

Access to information and protection of privacy are largely client driven activities. There is a very real ebb and flow to the volume of work as a result. That said, when the tide is high, public bodies need to have the resources, the internal knowledge and the flexibility to deal with whatever comes in the door. This includes a directive from leadership that, when necessary, priority is to be given to dealing with these issues.

One option which might help to address these issues is to create a centralized ATIPP Office within EIA which, in addition to taking the lead on policy and training with respect to access and privacy, would also take a leadership role in terms of responding to ATIPP requests made to all public bodies – while each public body would still have to search for and produce the responsive records, the central ATIPP office would do all the review and redaction. This would have several positive impacts. Firstly, it would create a group of access and privacy experts and specialists which would, in turn, result in more efficient and effective responses. It would allow employees to focus only on responding to access to information requests, rather than having to deal with their other job responsibilities. This would lead to far greater consistency in applying the exemptions under the Act. This would, in the long run, lead to fewer requests for review being made to the Information and Privacy Commissioner.

This group could also be responsible for privacy training throughout the GN. They could create and update as necessary, a mandatory on-line training program which would be required for all new or returning employees as well as advanced and specialized training for certain sectors (health, for instance). They could maintain a database of breaches which have occurred and incorporate “lessons learned” into new training

materials. We never learn from our mistakes unless we know what the mistake was and how it could have been avoided.

To be successful, however, this office would need to be given adequate manpower and resources. And, importantly, the remuneration offered for those who undertake these roles would have to be reflective of the importance of the work involved and the specialized training required so as to attract and keep those with the necessary expertise.