Office of the Access to Information and Privacy Commissioner
New Brunswick

Commissariat à l'accès à l'information et à la protection de la vie privée
Nouveau-Brunswick

ANNUAL REPORT 2013-2014

August 2016

The Honourable Chris Collins
Speaker of the Legislative Assembly
Legislative Building
706 Queen Street
Fredericton, New Brunswick
E3B 1C5

Dear Mr. Speaker,

Pursuant to section 63 of the *Right to Information and Protection of Privacy Act* and section 64 of the *Personal Health Information Privacy and Access Act*, I submit our fourth Annual Report, reporting on the activities of the Office of the Access to Information and Privacy Commissioner for the fiscal year of operations from April 1, 2013 to March 31, 2014. Thank you.

Respectfully submitted,

Anne E. Bertrand, Q.C.
Access to Information and Privacy Commissioner
/

Office of the Access to Information and Privacy Commissioner
New Brunswick

Commissariat à l'accès à l'information et à la protection de la vie privée
Nouveau-Brunswick

Annual Report 2013-2014
Table of Contents

FROM THE COMMISSIONER:

THE YEAR IN REVIEW

Having completed our fourth year of operations, we take this opportunity to reflect on the accomplishments, achievements and challenges we observed on both aspects of our Office's mandate: access to information and protection of privacy by public bodies, as well as the handling of personal health information in the health care system.

This year was another busy and interesting year at the Commissioner's Office, having received **547 files of all types and description**, and carrying from the previous year some 238 files, our case load was 785. Of those, we concluded a record number: 487, thus closing on average more than 40 files per month. The management of our files is described further in this Report, but needless to state that we gained invaluable experience in many respects throughout the entire year given this level of activity.

Public outreach continued to be an important component of our Office, as I was asked to give 16 presentations on the legislation while also giving 22 separate media interviews on our case investigation findings.

Under the *Right to Information and Protection of Privacy Act* alone, we opened 333 new files. Of that group of cases, 114 were access complaints to be added to the existing 42 cases we were already investigating. We resolved or otherwise concluded 107 of these complaints, requiring a tremendous effort in each case through our interactive process that focuses on education for the best application – and therefore, compliance with the *Act*'s rules.

Video surveillance in the public sector also garnered a lot of attention as municipalities and even schools considered their applicability and usefulness in their milieu. We developed a **Best Practice** on that subject alone and fielded a lot of inquiries on best approaches and how to lawfully install surveillance cameras in public areas as a last resort where all other security measures failed.

We also kept an eye on the number of access complaints being filed with the Courts instead of our Office (the other option allowed under the legislation), and there were only 2 during the

2013-2014 period. This meant that we remained relevant to the public, although the workload was causing more delays in the amount of time required to conclude our investigations.

As for our work in regards to the *Personal Health Information Privacy and Access Act*, we received 113 new files. All those cases required more time to resolve as health care providers who dealt with delicate workplace issues or grappling with notification to those affected by privacy breaches needed our guidance. Already handling in excess of 100 cases, in 2013-2014, we were none the less able to conclude 73 of the main files and kept the lines of communication open to pursue more results of internal investigations, undertake more research and develop helpful resources, while keeping an eye on implementation of corrective measures, and the like. Lack of training on rules surrounding access to personal health information and protection of privacy remained the biggest concern we noted in the public and privacy health care sector.

Although we noted improvements regarding compliance to both the Right to Information and Protection of Privacy Act and the Personal Health Information Privacy and Access Act, we recognized that much more needed to be done and that we could do more.

There were a number of Commissioner's Files that year on such subject matters as: the closure of retail store Zellers' and their pharmacies (to determine what would happen to client's health care information housed there); the conclusion to the major flood in Perth Andover in 2012 that had caused damage and/or loss of public and hospital records; leading an awareness of the need to apply the *Personal Health Information Privacy and Access Act* in public schools where school psychologists, school nurses and other health care providers handled student's health care information.

Other files that make up the numbers included our important public service to refer those who contact us but need other assistance (in 46 cases) and advisories to alert New Brunswickers of out-of-province privacy breach incidents that may affect them (2 major breaches in that year).

Although we noted improvements regarding compliance to both the *Right to Information and Protection of Privacy Act* and the *Personal Health Information Privacy and Access Act*, we recognized that much more needed to be done and that we could do more.

In that regard, we adopted a master plan regarding our processes that aim to assist public bodies and health care providers alike attain full compliance to this legislation by Year 5 of our mandate (2016). A lofty goal indeed, but one that enables us to remain focussed on the task at hand, and continue with our approach that is predicated on education and drawing attention to the benefits that come with compliance. In this Annual Report, we explore some of these achievements that we believe influence and encourage more progress.

Major case: Access to Information

In early 2013, the Provincial government announced plans to make significant changes to its public sector pension plan by adopting a shared risk plan. Amidst the concerns raised by those who would be affected by these changes, as well as media interest and a spirited public debate, the Province received a number of access to information requests under the *Right to Information and Protection of Privacy Act*. Our Office became involved when we received several complaints that required 49 separate rulings about how the Province had handled these requests, requiring us to investigate and issue findings in each case. This required us to be strategic and innovative in our approach to investigating related complaints involving several public bodies, with a view to conclude our investigations in a timely fashion. While the Province made some information available, most of the information was not disclosed. This case is explored more fully later in this Annual Report.

Major case: Protection of Privacy

On the privacy side, we also investigated a privacy breach matter concerning the disclosure of a student's personal information involving the Minister of Education and Early Childhood, his Executive Assistant, and Departmental officials. This case presented new challenges for our Office, given that the situation was already being publicly discussed: by the parents and the student who had spoken publicly about the situation, by the media, and by elected officials in the Legislative Assembly. The media, aware that our Office was investigating the matter, regularly asked for our investigation results.

While the case was being publicly discussed at the time, as our investigations are confidential until we share our findings at the conclusion of our work, we navigated delicately to get at the truth of the matter while being respectful of all parties and interests involved in the situation. In the end, we found that there had been a breach of the student's privacy and recommended measures to ensure that student information would be better protected in the future. During and after this investigation, we noted that privacy issues in the public sector could be raised for a different purpose: for political pressure or an attempt to discredit or punish those responsible. In our view, the reaction to this case showed a level of public distrust of government on privacy issues and a demand for accountability when it fails to protect privacy. This case is also explored more fully later in this Annual Report.

Privacy in the health care sector

The public's reaction to the privacy breaches in the health care sector was quite different than those involving government. Although involving highly sensitive information, privacy breaches in the health care sector generally attract less media coverage, have few political implications, and the public is more predisposed to excuse errors. Why? In our view, the public's main concern is timely access to quality health care services when they need them, and when personal health information is mishandled, it usually does not call the integrity of the health care system into question.

Newly subject public bodies

Having become subject to the *Right to Information and Protection of Privacy Act* in September 2012, municipalities, regional and municipal police forces, public universities, and schools and school districts were coming to terms with their obligations under the law. The public was asking them to provide more information, and expected more transparency about their operations and decision-making processes.

During our first investigations with these entities, we took this as an opportunity to learn about how they conduct their work, and to find solutions to help them adapt to their new obligations under the law. Municipalities, already familiar with various forms of regulation, were somewhat unsure how the law would impact their day-to-day operations, but we quickly learned that municipalities by nature are close to their citizens and accustomed to interacting with and providing the public with information. The concept of openness and transparency was already ingrained, and our work was instead focused on providing guidance on how best to effectively and properly apply the rules.

During the year, we:

- adapted our complaint investigation process for municipalities to make it more interactive and less formal, while still ensuring thoroughness of our investigations and compliance with the law;
- developed a master presentations and provided "train the trainer" type workshops for municipalities; and
- in June 2013, developed a public procurement guide to provide user-friendly directions on how to treat business and personal information collected during procurement processes.

Being truly committed to the success of both the *Right to Information and Protection of Privacy* and the *Personal Health Information Privacy and Access Act*, we came up with an internal 'MASTER PLAN' designed to encourage both the public sector and the public and private health care sector, step by step, to achieve full compliance within five years.

Progress in the Public sector

Since the start of our Office's mandate in 2010, we consistently reminded government to assist citizens when they want to know about projects, contracts, plans or decisions that may impact their lives, not only as a duty under the law, but as a key factor in successfully responding to access to information requests. In convincing public bodies to pursue this lofty goal, we took every opportunity to encourage them to adopt the following steps that would prove successful over time, including to:

- have discussions to ensure that they understood what specific information was being requested;
- keep the requesters informed as to when responses could be expected;
- conduct thorough searches for all relevant information before making a decision about access; and
- provide meaningful responses that include a list of all relevant records and helpful explanations if some information was not being provided.

Our experience has shown that where public bodies took these steps, requesters of the information were in a much better position to understand why access to some of the information they were seeking was not being provided, and were as a result, less likely to complain. We also remarked that in complaint cases where such steps had been taken at the outset, our investigations were more efficient; we could quickly assess if all relevant information had been identified and whether explanations for refusing access were justifiable.

We recognized that the public's right to know represents a cultural shift for government, requiring it to move away from protecting information to being more open and transparent by default, and we remained steadfast in encouraging the public sector to follow that path.

The 2013-2014 year proved to be somewhat successful as this message did resonate. We noted some improvement in the quality of the responses being provided during that year; however, there was still some resistance: not preparing lists of relevant records, not fully searching and retrieving all relevant information at the outset resulting in many cases having to ask public bodies to re-do their searches for us to be certain that all relevant information was identified. On the access to information front, we measured better outcomes:

- public bodies were increasingly meeting their duty to assist by contacting the requester and seeking a mutual understanding of what was sought and explaining when a response could be expected;
- public bodies moved away from the previous practice of using basic precedent letters in responding to access to information requests, and prepared more meaningful response letters that identified records and provided more helpful explanations if information was not being released; and
- public bodies were applying exceptions to disclosure only where required and more effectively, all the while giving reasons as to why some of the requested information would not be released in the circumstances.

Access complaint investigations outcomes

In the 2013-2014 year, the Office concluded 107 access complaints of which, 88 were cases where public bodies' response content was unsatisfactory

• 52 cases were resolved by public bodies accepting the Commissioner's recommended course of action and providing additional information

• 30 cases required the Commissioner to issue formal recommendations, and those were followed completely or in part, and by providing additional information

This left 6 cases where public bodies did not accept recommendations of the Commissioner

Overall outcome: 93% of cases where public bodies recognized and accepted that the public was entitled under the law to more information than initially provided.

Overall, we were pleased with the progress shown. In comparing our statistics with that of the Province, our Office received access complaints for only 9 – 10 % of all requests made across the Provincial government. For these reasons, we were optimistic that our Master Plan for full compliance in five year was attainable and we continued to embolden public bodies in this approach as a golden standard for the processing of all access to information requests.

Progress in the Health care sector

As for the health care sector, one of the major challenges was that several thousand New Brunswick health care providers were still not aware that they were subject to a law (the *Personal Health Information Privacy and Access Act*) that governs the handling of their patients' and clients' personal health information, despite it having been in effect since September 2010. We set this as a priority for the year. After identifying all of the professional organizations that licence health care providers operating in the Province, we then set out to find the most practical and effective way to reach them and to help them understand their obligations under the law.

Although we asked government for assistance to produce a training video, given our limited budget and staff resources, and while our mandate under the health legislation does not specifically include training, none was forthcoming. Undeterred, we developed a comprehensive presentation ("the Master Presentation") that set out all of the key concepts and obligations under the law. That fell well in line with our Master Plan to encourage the health care sector to achieve full compliance within five years. The Master Presentation was designed to break the law down into user-friendly rules and to provide practical examples of how best to apply the rules. As a starting point, we reminded health care providers that confidentiality and privacy of client or patient information is already well ingrained in their respective codes of professional conduct, and the new law simply codifies these rules into legal requirements.

Progress was more difficult to measure in this vast sector; however, we were very pleased to see that Regional Health Authorities embarked on more robust monitoring of privacy protection within their ranks, resulting in fewer breach notifications to our Office.

Overall, a respectable accomplishment and we could say with confidence… *en avant!*

Anne E. Bertrand, Q.C.
Access to Information and Privacy Commissioner for New Brunswick

PUBLIC OUTREACH, EDUCATION, AND AWARENESS

Presentations and Media Interviews

During 2013-2014, **the Commissioner gave presentations to 16 different groups** ranging from public bodies to university students, professional associations and healthcare providers, on the interpretation and best application of both the *Right to Information and Protection of Privacy Act*, and the *Personal Health Information Privacy and Access Act*: Association des Administrateurs Municipaux du N.-B., Recycle NB, WorkSafeNB Board of Directors, Medical Society's Community Hospital Program, Commission des déchets solides Nepisiguit-Chaleur, Executive Council Office-Women's Issues Branch, Lawyers and administrators at the Privacy Law and Compliance Conference in Toronto (Ontario), Union des Municipalités du N.-B., North York Community Homecare Inc., Provincial Government Right to Information Coordinators, UNB Faculty of Nursing, Department of Early Childhood Learning and Development, Village of Alma, Renaissance College in Fredericton (NB), Collège communautaire du N.-B. in Edmundston, Early Learning and Child Care Project Review Board of the Department of Early Childhood Learning and Development.

Investigators' Conference

Our Investigators and Intake Officers were invited to a cross-Canada Conference headed by the Privacy Commissioner of Canada which provided an excellent opportunity to discuss issues of common concern and share best practices. Benefits derived: fine-tuning our own processes to best deliver services.

The Commissioner also gave **22 media interviews** on complaints investigation findings.

Right to Know Week

September 23rd-28th, 2013

During Right to Know Week, the Commissioner's Office produced and posted more resources on its website, published ads in English and French daily newspapers in raising awareness about the public's rights, and the Commissioner gave presentations as indicated earlier.

Data Privacy Day

January 28th, 2014

A large mail out was undertaken to promote privacy with best practices, thematic calendars, and the Commissioner's Office's popular messaging bookmarks to government offices, universities, colleges, agencies, boards and commissions.

Comments on Proposed Legislation or Programs

When considering new legislation or a new program that may have implications for rights of access to information or raise concerns about the protection of privacy, public bodies may ask the Commissioner to provide input or comments. In 2013-2014, the Commissioner was asked to provide comments on 6 different proposed legislation and programs. This work was undertaken by a thorough review of the relevant background information and documentation, as well as through discussions with public body officials. As the media showed interest when made aware we had been asked to provide comments on a particular matter, the Commissioner developed a protocol specifying when it would be appropriate to comment publicly, with notice to government, particularly where concerns raised might not have been addressed fully.

****

RIGHT TO INFORMATION AND PROTECTION OF PRIVACY ACT

Breakdown of new files: 2013-2014

Between April 1, 2013 and March 31, 2014, the Commissioner's Office received **333** new files under the *Right to Information and Protection of Privacy Act*. The two largest types of files were General Inquiries and Access to Information Complaints.

General Inquiries (126)**:** when we receive a question from public and private associations, public bodies, interest groups, etc., seeking direction on the interpretation of the *Act*. Continued to be important numbers, with 20 prior, we answered 132 inquiries that year.

Access Complaints (114): include complaints when public bodies issue late responses to access to information requests, or when the applicant is not satisfied with the public body's response. In adding those to the 42 carried over from previous years, we were able to conclude 107.

Privacy Cases (37): added to 11 more cases carried over, those include concerns from individuals who believe their personal information was improperly handled, as well as self-reported privacy breaches by public bodies. We concluded 30 that year.

Time Extension Applications (18): when public bodies seek the Commissioner's authorization for additional time to respond to an access to information request, and those were concluded within a two week window.

Over the course of the year, we also continued to develop **Best Practices** to promote better understanding of the legislation. We also issued **Advisories** to notify New Brunswickers of events that can impacted their privacy by federal public departments.

AFTER THREE YEARS - The Sunset Clause

Section 5 of the *Act* created an initial 3-year transition period (ending September 1, 2013) that permitted provisions of other statutes to prohibit or restrict access to or disclosure of information, in addition to the rules under the *Act*.

While the *Act* was intended to be the primary statute that governs access to and disclosure of information by public bodies, the purpose of the transition period was to allow public bodies an opportunity to review their own legislation with a view to identify conflicts or inconsistencies between these statutes and the rules under the *Act*. If any were identified, public bodies had the opportunity to consider whether legislative amendments were required to prevail over the *Act*.

During the transition period, the Province passed a number of amendments to various statutes to add an express prevailing clause over the *Act*.

On September 1, 2013, subsection 5(2) came into effect, and the *Act* is now the prevailing law that governs access to information and privacy in the public sector. The only exception to this is where another Provincial statute is in conflict or inconsistent with the *Act*, and has an express provision that states that the other statute prevails over the *Act*.

In complaint cases where public bodies have relied on other statutes in refusing access to or disclosure of information, the Commissioner's Office will carefully examine the matter to determine which statute applies and whether it had been properly applied by the public body.

MORE ON PROGRESS…

Duty to assist and contacting requesters

Over the course of year, we noted that public bodies were contacting requesters of information shortly after receiving a request, particularly in cases where the request was not completely clear or was quite large in scope.

While public bodies understand their own operations and the language they use in their day-to-day activities, the average citizen usually does not and thus may not know how best to ask for a particular kind of information.

We were very pleased to learn that some public bodies were adopting this approach as part of their statutory duty to assist the public.

This approach was consistently encouraged as has been proven to:

- help both parties (the requester and the public body) understand and agree on what information is being sought;
- allow the public body the opportunity to explain what information it has in its records, which in turn may help the requester better focus or where amenable, narrow a request

to the specific information sought, particularly in those cases where unsure how to word the request;
- allows the public body to better understand what information the requester is looking for, which often allows a more efficient search for the relevant information and in turn, allows for more timely responses to be issued.

The Meaning of Seeking Clarification of Requests

Discussing the wording or scope of a request or where the requester agrees to modify or narrow the scope of his or her request, is not the same thing as seeking clarification. The public has the right to not agree to narrow the scope of one's request and the public body is obligated to respect this.

Rather, seeking clarification is a formal process under the *Act* and is used to manage unclear or vague requests for access to information, making it difficult and in some cases, impossible for public bodies to search for the requested information.

In fact, the *Act* requires those who seek access to government information to be as specific as possible in order to aid in the process of identifying where the requested information is kept, as a requirement to submitting a request.

THE PROCESS REQUIRED IN SEEKING CLARIFICATION: public body writes to the requester and asks that the request be made clear, following which the individual has 30 days to provide the requested clarifications. Where clarifications are not provided, the public body can choose to abandon the request as permitted under the *Act*; however, **notice to the individual is required**, along with informing of the right to complain to ensure that if there is disagreement, the Commissioner can review the case.

Meaningfulness of information provided by government

From the outset of our mandate, the Commissioner's Office has been consistently calling on public bodies to provide complete and meaningful responses to access to information requests, including:
- a list of all of the relevant records the public body has and reasons why access to any of this information is being refused, by indicating the specific exception to disclosure under the *Act* and helpful explanations as to why the exception applies to the information in question.

More importantly, a well-formulated response is put together with meaning, by using clear language, staying away from acronyms or expressions that are likely not used outside government circles, and fully answers the question put: ***I would like to know what information you have on this subject matter?***

A meaningful response to such a question goes a very long way in allowing the public to understand not only what information exists within government, but also in being able to appreciate what government is saying, what it is contemplating, and what it is going to rely upon to make decisions that impact its citizens.

A meaningful response is one that must make sense.

NEW GROUP ADDED TO RIGHT TO INFORMATION REGULATION

On September 1, 2012, a new group of public bodies became subject to the *Act*, including municipalities, regional and municipal police forces, firefighters, public universities, colleges, schools, school districts, regional service commissions. During the 2013-2014 fiscal year, we received complaints involving many of these new public bodies, and the Commissioner took this as an opportunity to meet with each public body to explain our role and investigative process, and to learn about how these public bodies conduct their work and could more easily adapt the rules under the law into their day-to-day work.

Municipalities

While some municipalities had been reluctant to be subject to yet another regulatory process, we only received very few access complaints over the year involving municipalities. While we are unsure how many requests municipalities had received over the course of the year, we note that there were approximately **125 municipal bodies** in New Brunswick at the time, and we know that some received a number of requests after becoming subject, while others did not receive any.

Observations from our first few investigations with municipalities:

- they were more likely to have contacted the applicant to acknowledge and discuss the request;
- their responses were overall helpful, listed relevant records and provided explanations for refusing access to any of this information;
- they tended to err on the side of caution if they unsure whether certain information could be disclosed (i.e., private sector business information).

We also noted that many municipalities were also already using their websites to proactively inform the public about their activities, including by-laws and policies, Council meeting minutes, budget information, staff salary information, etc.

Commissioner's process when complaints involve Municipalities

During our first investigations of complaints with municipalities, who were keen to learn more about how best to apply the Act but often had limited staff and resources, we quickly recognized the need to adapt our investigative approach, particularly for the smaller municipalities. Our goal was to make sure municipalities understood and would be able to meet their new obligations under the law with their existing resources and to minimize the impact of an investigation on their day-to-day operations. While conducting these investigations with the same level of thoroughness, we made the process more interactive and educational, and used the opportunity to provide guidance and direction on all aspects of processing and responding to access requests.

Universities

As for the public universities, they too were reluctant about becoming subject under the *Act*, and were the first of the newly subject public bodies to receive requests from the public, as well as complaints with our Office. Unlike the municipalities, the universities were less accustomed to making information about their operations available and having independent regulation and oversight.

The first requests for all public universities were for senior officials and staff salary and expense information, which had previously not been previously made publicly available. While the universities were initially reluctant to disclose this information in a way that would allow the public to fully understand how it compensated its officials and employees, we worked with them to help them better understand the transparency obligations under the law. In the end, all four universities began publishing salary and expense information on their respective websites.

Schools and School Districts

Schools and School Districts, much like municipalities, were also more accustomed to answering questions and providing information about their operations, which explains in part why our Office saw very little traffic on access complaints after they first became subject to the *Act*.

Community Colleges

As for the Province's community colleges, we also did not see many access complaints involving these public bodies, with the exception of one case where a person who had applied for job competitions was refused access to information contained in the community college's competition file. This was the first case where we investigated access rights to information in a competition file. Key findings: there existed a right of access to one's own competition information, including completed interview guide and evaluation results, although no right of access to information relating to other candidates' information. It appeared that the governing public procurement legislation provided more access that was taking place in practice and we brought that to the attention of government officials.

Access Complaint Spotlight - Case about access to information about the Shared Risk Pension Plan

After the Province announced its plans to amend its public sector pension plan to a shared risk model, six public bodies received access requests for information about the proposed changes: the Department of Finance, Justice and the Attorney General, Executive Council Office, Office of the Premier, Office of Human Resources, as well as the New Brunswick Internal Services Agency.

In May 2013, our Office began receiving complaints involving all six public bodies. The first complaints were about how the requests were initially handled: some requests had been transferred to other public bodies for response, some public bodies had self-extended the time limit to provide a response for an additional 30 days, and all but one of the public bodies did not respond within the statutory time limit to do so. As the public bodies began issuing their respective responses, we received further complaints as the Province had refused access to substantially all of the requested information, primarily as the final decision about how to proceed with changes to the public sector pension plan had not yet been made.

In total, we received 49 access complaints within a very short timeframe. To ensure that we thoroughly investigated all of these complaints in as timely a manner as possible, we developed a strategic investigation plan. As lists of records had not been provided in the responses, we asked that these be provided to us to facilitate our review of the relevant records and the reasons why access to most of this information had been refused.

Lessons learned:

Challenges for the public bodies:

- processing a broad access to information request during an already busy time of year—preparation of yearly budget submissions, Legislative Assembly was in session, plus a substantive amount of work involved in reviewing possible pension plan changes;
- public bodies having to consult amongst themselves, cross-referencing records to ensure that all of the relevant information had been identified and accounted for;
- all but one public body missed the statutory deadline to respond;
- overall reluctance by Government to give out further information than already made publicly available during the decision-making process, despite the fact that decision would have a substantial impact on New Brunswickers (both the public service that benefits from the pension plan, as well as the taxpayers).

- Overall findings:
  - Timeliness of response within set time limits not met;
  - Responses could have been clearer to allow a better understanding of what information existed and was not being provide;
  - Lack of a list of relevant records to enable better understanding of responses;
  - Some of the public bodies should have provided access to more information than initially provided but the legislation allowed most of the relevant information to be withheld, thus in compliance but less satisfactory outcome overall and the Province was not inclined to exercise its discretion in favour of more disclosure while final decision on how to proceed was still pending.

ABOUT *Self-reported Privacy Breaches*

A privacy breach occurs when personal information has been inappropriately collected, used or shared, or lost or stolen, or improperly disposed of, or worse, accessed by an unauthorized person.

While public bodies subject to the *Act* are responsible for privacy breaches that occur, they are not required to notify us of cases of privacy breaches (as are health care providers under the *Personal Health Information Privacy and Access Act*).

With the media attention garnered around previous cases, we noted that government bodies were more willing to notify our Office of breaches with a view to obtain our assistance, but more importantly, to ensure that an external, independent office investigated the cause of the privacy breach in order to report publically.

As a result, between April 1, 2013 and March 31, 2014, public bodies notified our Office of **14 separate cases of privacy breaches** regarding:

- Internal errors of misdirected mail
- Public bodies held responsible when external service providers from private sector hired to do its work but not handling sensitive information properly
- Unauthorized disclosure of personal information

Where public bodies notify the Commissioner that a privacy breach is suspected or discovered, we use the case as an opportunity to provide guidance and assistance to properly identify and address the cause of the breach, notify in a meaningful way those affected by the situation, and help establish appropriate measures to prevent recurrence.

Privacy Concerns

Members of the public who are concerned that a public body has mishandled their personal information can also contact our Office and ask the Commissioner to look into the matter. We refer to those cases as Privacy concerns, and between April 1, 2013 and March 31, 2014, we concluded **16 of such cases under *RTIPPA*.** We found that a few were **unfounded**, but only as a result of government's ability to use and share personal information without consent in one of its established program or activity.

OBSERVATIONS

- Reasons why individuals were complaining to us became clear: a lack of explanations given to them of government's intended or possible uses for their personal information at the outset, therefore leading to a poor understanding and raising issues of mistrust and concerns. Consent forms often too broadly worded and not sufficiently clear to allow full understanding as to how personal information would be collected, used, shared, etc.
- The need for training for employees and third party service providers to educate them on their obligations under the *Act* and the need to protect personal information at all times.

- Business information about a private company incorrectly considered under same rules that protect personal information under Part 3 of the *Act*. Business information subject to confidentiality considerations, privacy rights belong to individuals only.

Privacy Concern Spotlight: Case about a privacy breach in the education system

In August 2013, we released a Report of the Commissioner's Findings concerning the Department of Education and Early Childhood Development, and the disclosure of a student's results after completing the English Language Proficiency Assessment (ELPA, "the Assessment").

In this case, a student who had transferred to a New Brunswick school was required to complete the Assessment as part of graduation requirements. The purpose of the Assessment is to show that students graduating from Anglophone New Brunswick high schools have an acceptable level of literacy skills in the English language. Believing that the student had already demonstrated a high level of English proficiency so as not to need to complete the Assessment, the family raised the issue with the media, the school, the School District, the Department, as well as elected officials, including the then Minister. In the end, the student was required to take the Assessment in order to be considered for graduation that year.

When the test results were finalized, due to the high-profile nature of this case, a staff member of the Department notified senior Department officials that the student had taken the Assessment, and also disclosed the student's results. The Department officials then forwarded this same information to the Minister's Executive Assistant, who read the email aloud while at home and in earshot of another family member. The family member knew the student and immediately sent a congratulatory text message to the student, before the family had been made aware of the results.

Our findings showed that there were three privacy breaches in this case:

- the Department staff member was authorized to share that the student had taken the Assessment, but was not authorized to disclose the student's results in doing so, as this was more information than necessary under the circumstances;
- the breach continued when senior Department staff members relayed this same information to the Minister's Executive Assistant, which again did not require the disclosure of the student's results to inform that the student had taken the Assessment; and
- a third privacy breach occurred when the Minister's Executive Assistant read the email aloud at home with another family member within hearing distance.

The facts of the case showed that while everyone involved was primarily concerned about seeing a good outcome for this student, there was an overreliance on the fact that the family had sought assistance from various sources as an implied consent to share the outcome of the situation, including the student's results, and a mistaken belief that so long as the information was only shared amongst Department officials that it could not be a privacy breach. Further, the Minister's Executive Assistant should not have read the email aloud at home, given that other family members could have, and did in this case, overhear.

As a result, we issued recommendations that the Department and the Minister's Office review its internal practices to ensure that personal information is properly protected at all times, and that the Department follow the established practice for reporting students' Assessment results in all cases.

Our follow-up work to ensure these recommendations were implemented resulted in:

- Commissioner presenting a training session for Department officials on obligations under the law, and providing more direction to the Department and Minister's Office to improve its use of consent forms when individuals approach them for assistance.

PERSONAL HEALTH INFORMATION PRIVACY AND ACCESS ACT

Breakdown of new files: 2013-2014

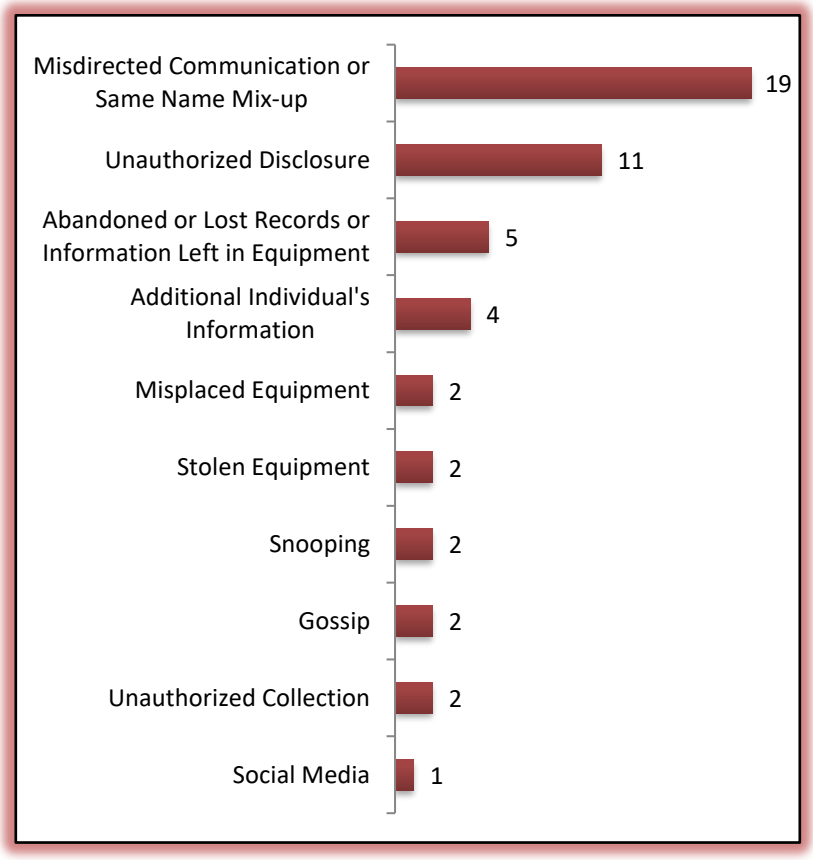
Between April 1, 2013 and March 31, 2014, our Office received **113** new cases under the *Personal Health Information Privacy and Access Act*. The majority of files were **Privacy Breach Notifications** (50), and **General Inquiries** (42 files), and **Complaints** (12)**.**

While the total number of files under this legislation being looked at that year was in excess of 220, we were able to conclude 82.

PRIVACY BREACH NOTIFICATIONS are mandatory under the *Personal Health Information Privacy and Access Act* for all public and privacy sector organizations, companies, professionals, including public sector health authorities and Department of Health ("custodians"), on the basis they handle health care information to dispense or assist in the delivery of health care in this Province. Notification is mandatory to both those affected and the Commissioner, whose oversight role ensures that the matter is investigated, and corrective measures put in place to reestablish and improve the protection of privacy.

Of these **50 new cases of privacy breaches notifications** (***shown on the accompanying graph***) reported to the Commissioner's Office, the majority involved **Misdirected Communication, Same Name Mix-up** or **Unauthorized Disclosure,** and the more troubling, snooping cases.

As a result of being notified, complaints were filed by those directly affected and we concluded 16 of those cases in that year.



Misdirected Communication or Same Name Mix-up is cases where personal health information of one individual shared with or sent to the wrong individual.

Unauthorized Disclosure occurs when personal health information was not intentionally disclosed to or shared with someone who was not permitted to see or know this information.

Unauthorized Collection is when more personal health information is collected than needed to carry out a specific task.

Abandoned or Lost Records or Information Left in Equipment incidents occurs when custodians cannot locate personal health information that should be in their custody, or when records are discarded inappropriately/improperly stored or destroyed, leaving them at further risk.

Breaches of **Additional Individual's Information** occur when another person's information was accidentally included along with information intended for another.

Misplaced Equipment breaches occur when equipment containing personal health information (like a USB stick or portable computer) is lost and later found, but raising questions as to access to the data.

Stolen Equipment is when the equipment is stolen and cannot be regained and the data is at risk.

Snooping refers to intentional act of accessing a patient or client's health care record without authorization, permission, or legitimate justification.

Gossip is when health care providers or their staff discusses patient/client information for a purpose other than the provision of health care (to those not supposed to be told of this information).

Social Media breaches are similar to Gossip or Unauthorized disclosure files that have specifically taken place over social media, like Facebook.

Privacy Breach Spotlight: Case about errors that resulted in the Department of Health issuing 114 Medicare cards to the wrong individuals and delays in processing new cards

In December 2013, the Department of Health notified the Commissioner of a privacy breach involving Medicare cards being sent to the wrong household addresses. At the time, the Department believed that as many as 153 individuals were affected; that number was later confirmed to be 138.

The cause of the breach was a malfunction in the Medicare database, which not only assigns individual Medicare numbers, but also a "household number" that allows the Department to send all Medicare cards to a particular household to the same address at the same time.

The database was designed to randomly assign a household number between 1 and 999,999, and to ensure that no two households would be assigned the same number. In December 2013, the household numbers automatically assigned reached 1,000,000, thus exceeding the maximum number of fields for the household number that the system could recognize. As a result, the household numbers in excess of 999,999 were automatically truncated to six digits, omitting the seventh digit. For example, numbers 1,000,001 to 1,000,009 were all read as 100,000.

After the household number is assigned with the corresponding Medicare numbers, this information is sent electronically to an external card manufacturer under contract with the Department. This information is used to produce the physical Medicare cards as well as the envelopes with the mailing address to ensure the cards are sent to the correct recipient.

In this case, as the household number sent to the card manufacturer was incorrect for all the Medicare numbers with a household number in excess of 999,999, this means that the address assigned to household number 100,000 received all of the Medicare cards for the household numbers that should have been recognized as 1,000,000 to 1,000,009, and so. Several households received Medicare cards for people who did not reside at that address, and many people who were waiting to receive their cards did not receive them.

When the Department discovered the cause and the extent of the breach, all production of Medicare cards was halted until the issue had been rectified. The cause of the breach stemmed back to changes that had been made to the Medicare system in 2011, at which time the Department recognized that the household numbers assigned by the system would, at some point in the near future, go past 999,999 and that changes needed to be made to prevent this from becoming an issue. While the system was then modified to increase the household number digit fields from 6 to 10, the necessary corresponding changes to ensure that the system would also send household number information in excess of 6 digits were not made.

The Department readily accepted that this was an oversight on its part, and our view, this situation could have been prevented had a full assessment of the implications of making this change to the Medicare database been undertaken before the changes were made. We found that conducting a privacy impact assessment would have helped the Department map out the necessary steps and conduct thorough testing, before making any changes, which would have allowed the Department to discover this to be an issue at the outset, instead of when things went wrong and several privacy breaches had already occurred.

Key lessons from this case: technology greatly facilitates many aspects of our lives, including in the delivery of health care-related services. Also requires public bodies that use technology to fully understand how it works and conducting thorough analyses to identify and address all possible issues that could arise when changes are being considered, particularly when it involves personal health information.

While the Department took all reasonable steps to retrieve the misdirected Medicare cards in this case, at the time of our last follow-up, 34 of the misdirected cards had not been accounted for, meaning that the breach could not be fully contained. Also, the disruption to the production of Medicare cards was an inconvenience for those waiting to receive them, as well as the Department, which had to dedicate significant resources to address the situation.

THE OFFICE: MANAGEMENT OF FILES

Comparing Previous Years

Compared to 2012-2013, more cases were brought to the Commissioner's Office and we opened **547** **new files under both legislation.**

A comparison of the last three years showed both growth but also efficiency in dealing with increasing case load every year.

Of the total 785 active files, 492 were concluded and closed in 2013-2014, meaning a performance measure of 63 percent output.

On average during that year, we concluded **41 files each month,** or **9.5 files per week.**

The files remaining active and having to be carried over to the next year necessarily increased in the last three years, but understandably due to a higher number and more complex incoming files as shown in the graph below.

These statistics demonstrated to us that despite the increasing workload, our Office was working more efficiently and better able to address the backlog of files that was unavoidably created when the Office was first set up in September 2010 with only three staff members.

Files carried over from previous year	New files received in 2011-2012	Total files being handled during 2011-2012	Files concluded in 2011-2012	Files carried into next year
78	512	590	456	134
Files carried over from previous year	**New files received in 2012-2013**	**Total files being handled during 2012-2013**	**Files concluded in 2012-2013**	**Files carried into next year**
134	531	665	426	239
Files carried over from previous year	**New files received in 2013-2014**	**Total files being handled during 2013-2014**	**Files concluded in 2013-2014**	**Files carried into next year**
239	547	785	492	294

Breakdown of Total Files Opened and Concluded

In total, **547** new files were opened in 2013-2014, with 17 Public Education, 22 Media interviews, 9 Commissioner's files, 2 Public Advisories, 46 Referrals, and in addition,

333 (or 61% of total) were matters involving the *Right to Information and Protection of Privacy Act*, and

113 (or 21 % of total) were opened under the *Personal Health Information Privacy and Access Act*.

Of those under the *Right to Information and Protection of Privacy Act* (added to the active files from previous periods), we were able to close:

- 132 General Inquiries
- 107 Access Complaints
- 19 Time Extension Applications to the Commissioner
- 16 Privacy concerns
- 14 Self-reported privacy breach cases
- 4 Requests to disregard
- 2 Public alerts
- 2 cases where complaints filed with Court

and under the *Personal Health Information legislation*:

- 45 General Inquiries
- 19 Complaints (3 Access to one's information and 16 Privacy)
- 9 Notifications of privacy breach cases

Concluding during that year a total of: **487 files**

Time to Concluding Investigations: *Right to Information and Protection of Privacy Act*

When our Office was created in 2010, one of our goals was to conclude investigations in a timely manner. The *Act* requires us to conclude investigations within 90 days, and allows us to extend the deadline by notifying the parties; however, that time constraint quickly became unworkable given our limited capacity and increasing workload. During the 2013-2014 year, we set a goal to conclude all investigations of access complaints within six months (180 days), with a view to be as timely as possible and to keep both applicants and public bodies on the same page in terms of when to expect us to complete our work. The result: **we came close to achieving our goal as our average turnaround time was 217 days (or approximately seven months).**

Time to Concluding Investigations: *Personal Health Information Privacy and Access Act*

While we concluded a lot of files under the health legislation, and as before, we found those matters to take significantly longer to conclude. The **Privacy Breach Notifications** concluded took the longest, on average 329 days. The reasons for this were the continued back and forth with those custodians who reported the breach to obtain the results of their own internal investigations. Those results were added to our own fact finding efforts to ensure a full picture as to what took place, along with an assessment of corrective measures proposed resulted in a lot of time spent on those matters.

SPECIAL MENTION FOR ACCESS COMPLAINT RESOLUTION UNDER THE *RIGHT TO INFORMATION AND PROTECTION OF PRIVACY ACT*

As with last year, our Office continued efforts to resolve complaints through our informal resolution process. Out the 107 access complaints concluded, with late or no response complaints dealt with by Intake Staff, we investigated in-depth the remaining 88 access complaints, specifically with the content of responses issued.

Success of the Access Complaint Resolution

Of those **88** access complaints**, 93% were resolved successfully** where various public bodies in government accepted to provide all of the information that should have been given in the first place to those who had requested it, during the Commissioner's resolution process or when deciding to follow the Commissioner's formal recommendations:

39 cases informally resolved without need to publish a Report of Findings, and

13 cases required a Report of Findings to publish findings without recommendations on the basis that those public bodies involved had agreed to provide all requested information during the complaint resolution process.

This meant that during 2013-2014, the Commissioner was required to issue in only **36** cases, formal recommendations, in published Reports of Findings or Reporting Letter for government to provide more information. Favorably, most of those cases resulted in success:

- **In 9 of these cases**, all of the recommendations were followed completely
- **In 21 cases,** the recommendations were followed in part (meaning some information was released, other was still withheld), leaving only,
- **In 6 cases**, where recommendations of the Commissioner were not followed.

Appeal to the Courts when Commissioner's recommendations not followed

Where any public body decides not to follow a recommendation of the Commissioner issued at the conclusion of a complaint investigation, there is an automatic right of appeal to the Court of Queen's Bench. Our Office tracks whether appeals have been filed, and if so, their outcomes. There was only one court decision during 2013-2014, that of **F-M-41-2013 involving the Department of Energy.** The Court issued an **Interim Order** after its hearing of September 18, 2013 **upholding** the Commissioner's recommendation that the Department provide to the Applicant a list of all relevant records and corresponding explanations where information was being refused. The case was later settled without further determination by the Court.

THE COMMISSIONER'S TEAM IN 2013-2014

The Office of the Access to Information and Privacy Commissioner benefitted from the valued work of a team of dedicated individuals:

Legal Counsel and Investigators

Kara Patterson

Chantal Gionet

Anik Cormier

Intake and Portfolio Officers

Norah Kennedy

Lucrèce Nussbaum

FINANCIAL INFORMATION - fiscal year March 31, 2014

Total Expenditures 590 650

Wages & Benefits	494 000	Rent	48 050
Office	15 700	Translation (decisions, resources)	18 100
Travel (investigations and training)	11 500	Legal fees (court case)	3 300

Have Questions or Concerns? *Please Contact Us:*

Office of the Access to Information and Privacy Commissioner
New Brunswick

Commissariat à l'accès à l'information et à la protection de la vie privée
Nouveau-Brunswick

65 Regent St. Suite/bureau 230
Fredericton, NB E3B 7H8

☎ 506-453-5965 | Toll-free: 1-888-755-281

Access.info.privacy@gnb.ca |Acces.info.vieprivee@gnb.ca

www.info-priv-nb-ca