Manitoba Ombudsman

2013 Annual Report under The Freedom of Information and Protection of Privacy Act and The Personal Health Information Act

Upholding your Access and Privacy Rights in Manitoba

Message from the Ombudsman

Fulfilling our statutory mandate requires action on many fronts in addition to our core oversight function of investigating complaints about access to information and breaches of privacy. I am proud to report that in 2013 Manitoba Ombudsman once again engaged in a broad range of activities intended to strengthen the access and privacy rights of Manitobans, including consultation or commenting on proposed policies that affect privacy rights, as well as education and training for the public and public bodies.

2013 brought with it a series of interesting complaints and issues for investigation, some of which are highlighted later in this report. In one case, we considered whether a public body could refuse access to information about its contract with a private company for the provision of services, and determined that most of the information should be released.

In other cases, we looked at whether an employee's emails that were of a solely personal nature were in the custody or control of the public body as a result of being sent on the employer's electronic network – we concluded that they were not, and that the emails did not constitute a collection or disclosure of personal information by or for the public body. We also looked at whether a personal opinion expressed in an email could be withheld on the basis that disclosure could reveal "advice, opinions, proposals, recommendations, analyses or policy options developed by or for the public body or a minister" and concluded that the information in the email did not fall into any of these categories and should not have been withheld (this case was discussed in our 2013-3 issue of *OmbudsNews*).

We also saw a small number of troubling instances of privacy breaches arising from health care employees "snooping" in electronic records of highly sensitive personal health information. It was reassuring to see that trustees took these matters seriously and that improvements were and are being made to prevent similar breaches in the future.

Among the variety of complaints and issues we saw, one thing was constant – the issues continue to increase in complexity, requiring corresponding increases in time for research and investigation. More than ever before, the cooperative working relationships that we have with public bodies and trustees are crucial to our ability to serve the public by conducting comprehensive and timely investigations.

Our redesigned website was launched in March 2013 to reorganize and expand content and improve navigation. In addition to traditional tools such as our practice notes we now routinely post FIPPA investigation reports on our website. The reports posted in 2013, reflecting the important matters about which information was requested through the access process, demonstrate the use made of the legislation and its value to the public. The reports also demonstrate the efforts – the successes and failures – of public bodies in responding to access applications from the public. Our investigation reports can also be an education tool for the public and public bodies, providing insight into how Manitoba Ombudsman interprets and applies the legislation and resolves complaints in situations where recommendations are not required.

In 2013 we also began using Facebook and YouTube to share information and increase public awareness of issues. We posted videos about exercising health information rights in relation to eChart Manitoba and more generally, about how to request access to personal health information under PHIA, as well as about accessing information under FIPPA, among other topics.

These new steps were in addition to our more traditional educational activities such as presentations and publications for both the public and public bodies and trustees. With the expansion of eChart Manitoba in 2013 we produced and distributed a new brochure, *Know Your Health Information Rights*. This brochure was produced in consultation with Manitoba eHealth, who also undertook to distribute the brochure to eChart sites throughout Manitoba. We also distributed the brochure through municipal government offices and other community organizations in Manitoba. Other resources for the public included tips and presentations on fraud prevention, as well as our popular "Guard Your Card" credit and debit card shields designed to protect chip cards from unauthorized scanning.

In May 2013, we hosted two conferences to strengthen the access to information and protection of privacy system in Manitoba by helping employees of public bodies and trustees meet today's information challenges.

The world of access and privacy is a complicated tapestry with technology increasingly interwoven with, and sometimes driving, policy and practice in areas such as records management and security. Participants in our Access, Privacy, Security and Information Management Conference included public sector employees from provincial and municipal governments, school divisions, universities, colleges and health-care bodies. The theme of the conference, Making Connections, reflected the interrelationships between information access, privacy, security and records management.

Also in 2013, Manitoba Ombudsman, together with the offices of the information and privacy commissioners in Saskatchewan, Alberta and British Columbia, co-hosted the Western Canada Health Information Privacy Symposium in Winnipeg. Trustees, including health professionals and employees who handle personal health information in regional health authorities, hospitals and other health-care facilities, discovered how individuals and organizations in the four western provinces have successfully addressed common health information privacy issues and challenges.

As the access and privacy oversight office under FIPPA and PHIA, Manitoba Ombudsman is part of a federal, provincial and territorial community of oversight offices. Participating in the discussion of larger access and privacy issues allows us to ensure that Manitoba's perspective on these issues in not overlooked. Being part of the community also allows us to benefit from the work done and knowledge gained by other jurisdictions; knowledge we can then share through events like the conferences hosted in 2013.

During 2013, oversight offices in Canada collaborated to promote national and international initiatives such as Data Privacy Day and Right to Know Day, which raise public awareness of access and privacy rights. I also met with my Canadian colleagues at a forum to discuss issues of mutual concern, including the impact of evolving information communication technologies on access and privacy rights and information management practices. Emerging from this meeting was a joint resolution urging governments to ensure that Canadian laws are strong enough to address the challenges posed by dramatic technological change and expectations of engaged citizens.

The greatest challenge for proponents of better access and privacy laws, including legislators and oversight offices, continues to be our ability to create effective and accessible laws, policies, and procedures in the face of rapidly changing technology. Recognition of the interconnectedness of access and privacy regimes with security systems and information management practices, will enable us to serve the public effectively in a continuously evolving digital age. I believe the work we are doing in Manitoba ensures that we will not be left behind, and I am proud of Manitoba Ombudsman's leadership role in that work.

The Honourable Daryl Reid
Speaker of the Legislative Assembly
Province of Manitoba
Room 244 Legislative Building
Winnipeg, MB R3C 0V8

Dear Mr. Speaker:

In accordance with subsection 58(1) of *The Freedom of Information and Protection of Privacy Act* and subsection 37(1) of *The Personal Health Information Act,* I am pleased to submit the annual report of the ombudsman for the calendar year January 1, 2013 to December 31, 2013.

Yours truly,

Mel Holley

Mel Holley
Acting Manitoba Ombudsman

In Winnipeg:
750 - 500 Portage Avenue
Winnipeg, MB R3C 3X1
204-982-9130
1-800-665-0531 (toll free in Manitoba)
Fax: 204-942-7803

In Brandon:
202 - 1011 Rosser Avenue
Brandon, MB R7A 0L5
204-571-5151
1-888-543-8230 (toll free in Manitoba)
Fax: 204-571-5157

On the web:
www.ombudsman.mb.ca
www.facebook.com/manitobaombudsman

Access and Privacy Cases of Interest

Just the facts

Individuals have a right to request corrections of any errors or omissions in their personal or health information held by public bodies and trustees. This is an important right, giving people the opportunity to ensure that information about them is accurate and complete. Some cases in the past year required us to consider the definitions of both "correction" and "error."

For example, in a case involving the Winnipeg Police Service (WPS) an individual described as a "witness" to an alleged crime wanted his name removed because he was not in fact a witness. The WPS changed the description from "witness" to "other," a designation that includes people who may be interviewed at some point. In this case the name of the person was given to police by the alleged victim who indicated that this person may also have witnessed the crime.

We concluded that the change from witness to "other" was an appropriate correction which made the information accurate, but that in the circumstances the inclusion of the name in the file was reasonable and there was no basis for removing it entirely. In this case what the person wanted was a deletion, not a correction.

In another case, a tenant took issue with the characterization of some of her actions contained in the file of her public housing landlord. Our investigation concluded that the characterization of an exchange, in a record created by one party to the exchange, was not a factual error that could be corrected in the manner contemplated by the legislation.

The tenant in that case had expressed concern that information in her file would cast her in a negative light and if not corrected could ultimately be used against her. We understood her concern and while we could not agree that a correction was required in this case, we noted that there is a provision under FIPPA that enables people to effectively add their own comments to the disputed information about them. When a public body refuses to make the requested correction, it must add the individual's request for correction to any record of that information in its custody or under its control. This ensures that the individual's perspective on the disputed information is connected to and read with the actual information when someone looks at the record.

Under PHIA, when a trustee refuses to make a requested correction, the individual can provide a statement of their disagreement about the information which must be added to the disputed information. In a previous case we investigated, a person sought the correction of what he felt was an error in his medical file. What he considered an error was in fact a medical opinion expressed by a physician. The accuracy of the information on which the medical opinion was based did not appear to be in dispute. We concluded that the disputed information was a professional opinion and not an error of fact and therefore the trustee's decision not to correct the record as requested was reasonable.

The correction rights under PHIA and FIPPA enable individuals to challenge the accuracy and completeness of information held about them, and in circumstances where corrections are not made, individuals are able to have their position added to the record to balance what they consider to be errors or omissions.

The big search

In accordance with FIPPA, public bodies have a duty to assist applicants making a request for access. One of the most important ways a public body can ensure it meets this requirement, particularly with wide-ranging requests that might impact their operations or result in excessive costs to the applicant, is to work with applicants to see if such requests can be narrowed while still providing the applicant with the information they are entitled to receive.

Manitoba Ombudsman encourages both applicants and public bodies to engage in open communication and to act reasonably in an effort to meet the spirit and intent of the legislation.

Advances in technology have generally allowed for the quick retrieval of vast amounts of data with minimal effort and cost. But that is not always the case, as demonstrated in our investigation of a complaint against the Winnipeg Police Service (WPS).

The applicant had requested all documents and emails between 2009 and 2012 that referenced or mentioned his name or the name of his group. It was clear to the WPS that significant costs would be associated with such a wide-ranging request. Normally the next step for a public body would be to issue a formal estimate of costs for such a request. But in this instance, the WPS took a different approach. Instead of issuing an estimate of costs, they took the step of issuing a letter detailing the amount of time that would be involved in various aspects of searching for responsive records. We were advised that this was done in an effort to help the complainant understand the process and potential costs involved in processing his request and to provide him with an opportunity to modify his request.

The WPS advised the complainant that if the request was not narrowed, it would have no option but to refuse access in full as processing the request in its current scope would unreasonably interfere with the operations of the WPS. The applicant questioned the reasonableness of the position taken by the WPS and complained to our office.

In the course of our investigation the WPS provided a detailed description of the steps involved in the necessary restoration and search of back-up files in order to locate the requested emails. This included an estimate of the number of files, volume of data, and rate of restoration. We reviewed and analyzed the estimates and ultimately we concurred with the WPS estimate that it would involve 30 days to restore data from past and present servers and almost 16,000 hours to examine the files for relevant emails. Clearly, based on the volume of information and data, and the rate of restoration and search time required, even locating the responsive email records would not be feasible.

The WPS also detailed for the applicant specific areas within the service that would be more likely to have responsive records than others. Targeting these areas was also a potential option available to the complainant, but one he chose not to exercise.

In this matter, we were satisfied with the efforts of the WPS to meet the duty to assist requirement. The WPS made an effort to provide the complainant with information to help explain the costs involved with his request and possible ways to narrow the search. It serves as a good example for all public bodies that there may be different ways of fulfilling their duty to assist FIPPA applicants, and a caution to applicants that despite advances in technology not all electronic record searches can be done in an expeditious or cost effective manner.

A fair vote

The 2012 merger of regional health authorities in Manitoba resulted in changes for some of the province's largest labour unions. Because of the amalgamation, certain bargaining units were, in effect, represented by two unions. By law, only one union can represent one bargaining unit so the affected workers had to choose which union was going to represent their interests. Conducting the vote, however, proved to be a challenge which ultimately led to a complaint to our office.

The dispute involved employees in a professional/technical paramedical capacity in the newly-created Western Regional Health Authority. Some of those workers were represented by Manitoba Association of Health Care Professionals (MAHCP) while others belonged to the Manitoba Government and General Employees' Union (MGEU).

The Manitoba Labour Board ordered that a representation vote be held and provided the names of all the affected workers to the two unions but not their home addresses. MAHCP subsequently made a FIPPA application to the board for access to the employees' home addresses, which led to the refusal of access complaint to our office.

MAHCP argued that access to the home addresses was necessary for a fair vote. The union claimed it needed the addresses to contact and communicate to employees the benefits of belonging to a particular union so the workers could make an informed choice as to their designated representative.

The board cited several grounds under FIPPA for refusing access to the personal information: the highly sensitive nature of the information, possible harm arising from the release of the addresses, and the release of the information would be inconsistent with the purpose for which it was collected.

We acknowledged that the personal information requested – an individual's home address – can be highly sensitive information, as disclosure of this information in some circumstances could cause serious personal distress and has the potential to violate personal security by facilitating physical contact with individuals at their homes. However, our investigation could not conclude that releasing the addresses to unions wishing to contact workers at home to solicit their support would cause serious personal distress to workers or otherwise expose them to harm.

FIPPA favors withholding personal information if the disclosure would be inconsistent with the purpose for which the information was obtained. In this case, employees' home addresses were collected by the board to fulfill its statutory mandate, that being to facilitate the representation vote. The board maintained that providing the home addresses to the union for campaigning or electioneering purposes was not consistent with the board's purpose for the collection of the information. Our office agreed. In doing so we also noted that the board's refusal to provide access to the home addresses did not preclude either union from communicating or contacting employees by other means.

This complaint underscored the complexity of applying access and privacy legislation within the framework of a labour relations regime. In this case, our office was tasked with ensuring that the access decision of the board was compliant with FIPPA while at the same time recognizing the board's expertise in interpreting and applying its own statutes, particularly with respect to determining what constitutes a fair vote. Ultimately our office supported the decision of the board to refuse access to the home addresses.

You've got mail

Sending and receiving email has become part our daily workplace routine. In some situations, email is used in the workplace to communicate important and sensitive information to both internal and external parties. The need to be cautious when sending sensitive personal information by email was reinforced when an employee's privacy was breached at a Manitoba public body after an email containing personal information related to the recipient's employment status was unintentionally transmitted to all staff. Clearly such a disclosure had the potential to cause significant harm and/or humiliation to the employee whose privacy was compromised.

Our investigation of the breach revealed that an email containing personal information was first sent to the employee with an extra address in the "to" field of the email that represented a distribution list. The distribution list address had been added by the sender accidentally. While the initial email was not distributed widely as the sender did not have the authority to send emails to that specific distribution list, when the employee selected "reply to all" when responding, the email was transmitted to everyone on the list since the employee did have the authority to send to the list.

We concluded that the public body made appropriate efforts to contain the breach and notify the employee whose privacy was compromised.

The public body also took reasonable measures to mitigate future risks to privacy, including those associated with the use of large distribution lists.

Our findings in this matter, however, provide valuable lessons for both employees and managers of public bodies when it comes to using email in the workplace, including:

- Send with care. In the event that sensitive, personnel-related information needs to be sent via email for any particular purpose, eliminate wherever possible any identifying information (names, addresses, etc.) from the emails.
- Limited capability. Consider limiting the number of staff within the public body to only those that need to transmit email to "all staff."
- Don't leave it on the shelf. Training/education and awareness of relevant policies and legislation is important. In this matter resources (such as policies on network usage, managing email, etc.) were available to provide guidance and direction to employees who use the public body's electronic network. The employee who transmitted the email to all staff in this case was new to the position and had not been made fully aware of the resources available.

Open for business

Public bodies routinely enter into contracts for the provision of goods and services by the private sector. Contracts and other business matters involving public bodies are of considerable interest to the public, who often have questions about the costs of goods and services, the impact of potential changes to the delivery of goods and services, or about how successful bidders have been selected. As with most other documents in the custody or control of public bodies, business contracts and other related records are subject to the right of access under FIPPA, and must be disclosed to an applicant unless an exception to access applies to the record or information in the record.

In this case, we were asked to investigate a decision by the University of Manitoba to withhold its entire contract with Xerox Canada for the provision of managed print services. The university initially intended to release some information from the contract, but after consulting with Xerox and hearing Xerox's objections, the university concluded that disclosure of any portion of the contract would harm Xerox's business interests, and that it was required to withhold the entire contract under FIPPA.

Our investigation revealed that a considerable amount of information from the contract could be discovered from public sources, such as the websites of both the university and Xerox. When we brought this to the university's attention, the university agreed to release this type of information to the applicant.

However, much of the information in the contract continued to be redacted. Upon our review of the evidence we were unable to conclude that releasing information such as standard contractual terms or general information about managed print services would be harmful to Xerox's business interests. Ultimately, we concluded that only the detailed cost projections and the detailed process descriptions were required to be withheld under FIPPA. The ombudsman recommended that the university release all of the remaining information in the contract to the applicant, and the university complied.

This case illustrates the point that public bodies and their business partners can expect to be subject to public scrutiny. The legislation establishes a balance between protecting competitive business information and the transparency required to sustain confidence in public bodies when dealing with private contractors. Ensuring that decisions of public bodies respect that balance in a manner consistent with the spirit and intent of the legislation is one of the roles of Manitoba Ombudsman as an oversight office.

In this case it was clear that upholding a refusal of access to information that was, in part, already publicly available from the parties, or standard contractual terms and general information, was not consistent with the intent of the legislation.

For details of our investigation and findings, see our report with recommendations available on our website.

Whose record is it?

Public bodies, like many employers, are increasingly adopting policies that permit employees to make limited personal use of an employer's electronic network.

Our office investigated an allegation that a complainant's personal information had been inappropriately collected and disclosed by a public body when an employee of the public body (his ex-spouse) used her work email to send and receive personal communications pertaining to the complainant.

In order to determine whether the public body was responsible for the collection and disclosure of the complainant's personal information in these emails, we first had to establish whether or not the emails were in the custody or control of the public body for the purposes of FIPPA.

There was no question that the employee had sent and received some emails containing the complainant's personal information. And, given that the emails were stored on the public body's email server, it appeared obvious that they were in the public body's possession. However, the emails were of an entirely personal nature, completely unrelated to the mandate and functions of the public body.

The public body in this case explained to our office that its employees are permitted limited personal use of its electronic network, including email, pursuant to its Acceptable Use Policy. The public body further explained that employees have an expectation of privacy in their personal email communication and that it does not consider personal email to be part of its "official" communication. There was no reason for the public body to conclude that its Acceptable Use Policy had been breached by the employee.

Since the records in question were not created by the public body employee in the course of her work-related duties and the contents of the records did not relate to the public body's function or business operations, our office concluded that although the email records were stored on the public body's email server, it did not have custody or control of the employee's personal emails for the purposes of FIPPA. As a result, the emails are not subject to the application of FIPPA.

Do they really need to collect my personal information?

Public bodies often require personal information in order to deliver programs and services. Before asking for personal information, public bodies should carefully consider what personal information they really need to collect. If the collection is determined to be necessary, the public body has an obligation under FIPPA to inform individuals about its reason(s) for collecting the information.

Manitoba Ombudsman investigated a matter in which several City of Winnipeg employees believed that too much personal information was being collected by the Winnipeg Parking Authority (WPA) in order to issue parking permits. The employees believed that the personal information already provided to the WPA (name, contact information, employee number, make of car, and licence plate number) was more than sufficient to issue parking permits. The WPA, however, also requested their driver's licence numbers.

The WPA initially explained to the ombudsman that the collection of driver's licence numbers was necessary in order to eliminate duplicate accounts. Having driver's licence numbers would allow the WPA to merge information relating to parking tickets and parking permits into one account. Some complainants indicated, however, that they were told that collection of driver's licence numbers was necessary to confirm home addresses.

During the course of our investigation, it became clear through discussions with the WPA that the personal information in question was being collected by the public body to carry out its responsibilities concerning enforcement, specifically the collection of fines for parking-related offences.

The WPA indicated that it is their policy not to issue parking permits to applicants if they have outstanding parking fines and to cancel the permits of those who fail to pay any monies owed. The WPA advised our office that it requires driver's licence numbers in order to accurately determine if an individual has outstanding fines, as it is the only unique identifier for the enforcement program.

As result, we concluded that the collection of driver's licence numbers was in accordance with FIPPA as the information collected related directly to and is necessary for an existing service, program or activity of the public body.

But that was not the end of it. When a public body collects personal information directly from the individual the information is about, it must inform the individual of:

- the purpose for which the information is collected,
- the legal authority for the collection, and
- the title, business address and telephone number of an officer or employee of the public body who can answer the individual's questions about the collection (subsection 37(2)).

In this case, notice about the collection of personal information on the WPA parking permit application was not provided. We advised the WPA of the requirements of FIPPA. As a result, all parking permit applications, including those for the general public, now include a notice of collection in accordance with the act.

This case can serve as a reminder for public bodies to ensure the personal information they collect is necessary to carry out their duties and to make sure this collection is explained to those required to provide the personal information.

Reaching Out

During 2013 we reached out to the public to promote an understanding of access and privacy rights under FIPPA and PHIA, and to public bodies and trustees to promote statutory compliance and best practices. Our outreach activities included making presentations, participating in events, and sharing information through our print publications, website, Facebook page and YouTube videos.

To raise awareness of the impact of technology on privacy and to promote the importance of protecting personal information, we marked international Data Privacy Day on January 28, by:

- providing tips for the public to protect their personal and personal health information
- making ID shields available for credit and debit cards that can be waved or tapped to make a payment due to having radio frequency identification (RFID) chips containing our personal information
- distributing a series of three bilingual posters, as a joint effort by federal, provincial and territorial privacy commissioners, which promoted the theme, "Take control of your information. Don't let it come back to haunt you."

For Fraud Prevention Month in March, we created an identity theft web page with links to various resources to inform Manitobans of steps they can take to protect their personal information and what to do if they are the victim of identity theft or fraud.

Right to Know Day, celebrated around the world on September 28, acknowledges an individual's democratic right of access to government-held information and promotes the benefits of open, accessible, and transparent government. To foster awareness of the right to know, we posted three new videos on our YouTube channel. The first video, Exercise Your Right to Know, talks about why this right is important. The other two videos are "how to" videos that focus on accessing information under Manitoba's *Freedom of Information and Protection of Privacy Act* and accessing personal health information under *The Personal Health Information Act*.

We gave presentations on various topics to the public, public bodies and trustees, including:

- two presentations to the public on protecting their personal information from identity theft
- participating in a half-day training session about FIPPA for local public bodies, including employees of local government bodies, educational bodies and health care bodies
- presenting at PHIA Day at the Southern Health Authority on privacy breach prevention and key steps for responding effectively to a breach
- delivering Brown Bag Talks to access and privacy personnel in public bodies and trustees
- presenting on access and privacy topics at two conferences that we hosted
- speaking with legislative interns and staff of Elections Manitoba about our mandate and duties.

Along with other provincial and territorial privacy oversight offices, we participated in the development of the Privacy Commissioner of Canada's Privacy Emergency Kit to help public and private sector organizations subject to federal, provincial and territorial privacy laws plan for the handling of personal information before an emergency strikes. Uncertainty about the sharing of personal information during an emergency such as a flood, fire or tornado, can result in delays and have significant consequences for people. The kit is intended to facilitate timely information sharing during an emergency and enhance public confidence that personal information will be handled appropriately. It includes frequently asked questions about the legal authority for sharing personal information as well as checklists for appropriate handling of personal information before, during and after an emergency.

We developed a brochure to make Manitobans more aware of their health information rights in relation to the provincial electronic health record system, eChart Manitoba (see separate article).

Our office participated in Law Day and spoke with the public about the ombudsman's role and provided information and brochures about FIPPA, PHIA, *The Ombudsman Act* and *The Public Interest Disclosure (Whistleblower Protection) Act*. We also staffed

informational display booths at the Association of Manitoba Municipalities' Annual Convention, the Manitoba Social Sciences Teachers' Association Conference, and the Rural and Northern Health Day hosted by the Manitoba Centre for Health Policy.

With assistance from advisory committee members, we organized two conferences that brought together employees of public bodies and trustees to share solutions for today's information access and privacy challenges (see separate article).

In our quarterly newsletter, *OmbudsNews*, we featured articles about protecting personal information, the risks and precautions concerning the use of email and the importance of the privacy role of access and privacy coordinators.

We launched our redesigned website, which expands the information we make available to assist the public in understanding and exercising their access to information and privacy rights and finding out how our office can help them with concerns and complaints. The Access and Privacy Division pages were reorganized into two separate groupings of FIPPA and PHIA-specific information, tools and resources, to facilitate locating act-specific information.

Through our Facebook page, we shared information to promote awareness of access and privacy issues and trends.

Since 2011, we have been posting investigation reports that contain recommendations as well as a summary of the public body's/trustee's response to the recommendations. During 2013, we began posting selected investigation reports in cases which did not require recommendations, in order to increase transparency of our investigations and provide insight into our analysis and interpretation of provisions of FIPPA and PHIA. We began by posting 21 investigation reports in 2013.

2013 Access and Privacy Conferences

In May 2013, we hosted two conferences to strengthen the information access and privacy system in Manitoba by helping employees of public bodies and trustees meet today's information challenges. Advisory committee members representing public bodies and trustees participated in developing the agendas and planning the conferences. Participants in each two-day conference heard from experts from Manitoba and across Canada in sessions and workshops aimed at fostering best practices and compliance with legislative requirements under FIPPA and PHIA.

Participants in our Access, Privacy, Security and Information Management Conference included public sector employees from provincial and municipal governments, school divisions, universities, colleges and health care bodies. The theme of the conference, Making Connections, reflects the interrelationships between information access, privacy, security and management. For example, strong security safeguards for information enhance the protection of privacy and effective information management facilitates timely access to information.

The conference provided participants with opportunities to learn about embedding privacy-protective measures into the design of programs and systems and developing options to provide access to information through open data and proactive disclosure initiatives. Sessions delivered practical advice on mitigating security risks, overcoming privacy challenges, responding to access requests and managing information in a digital environment.

Also in 2013, Manitoba Ombudsman, together with the offices of the information and privacy commissioners in Saskatchewan, Alberta and British Columbia, co-hosted the Western Canada Health Information Privacy Symposium in Winnipeg. Trustees, including health professionals and employees who handle personal health information in regional health authorities, hospitals and other health-care facilities, discovered how individuals and organizations in the four western provinces have successfully addressed common health information privacy issues and challenges.

The symposium delivered practical guidance on building and maintaining successful health information privacy operations and dealing with privacy issues and challenges, including privacy breaches. Advanced topics included emerging trends and technologies, cross-jurisdictional privacy issues and health information privacy and research.

Panel presentation (L-R): Nancy Love (MB Omb), Diane Aldridge (SK OIPC), Brian Hamilton (AB OIPC)

Three of your WCHIPS hosts (L-R): Gary Dickson, former Information and Privacy Commissioner of Saskatchewan, Jill Clayton, Information and Privacy Commissioner of Alberta, Mel Holley, Acting Manitoba Ombudsman

A conference session

Promoting Privacy Awareness of Health Information Rights

The ombudsman's role under PHIA includes informing the public about their rights under the act.

To enhance Manitobans' awareness of their health information rights under the provincial electronic health information system named eChart Manitoba, we published a brochure outlining six rights that can be exercised. We also created a YouTube video that explains these rights.

EChart pulls together existing electronic health information already collected at different points of care, including prescriptions filled at retail pharmacies, immunizations, test results from participating labs, diagnostic image reports, and personal identifying information such as personal health identification numbers, birth dates and addresses.

Some personal health information of all Manitobans is available to authorized health-care providers and their support staff through eChart. At the time our brochure was published, the personal health information of Manitobans contained in eChart was available to over 10,000 authorized users in over 260 health-care sites throughout the province, such as medical clinics and hospitals.

Authorized eChart users can search, view and print personal health information from eChart. There are different levels of access based on the users' need to know the information to perform their jobs. For example, a physician may be able to see all of your information, while reception staff may only have access to information such as your name, address and PHIN. The system does not restrict the user to viewing only his or her patients' personal health information. Each user has a unique username and password to access the system and all access to eChart is logged (recorded) and is subject to audits.

Our brochure has been distributed to eChart sites by Manitoba eHealth. Our office distributed the brochure to municipal government offices and community organizations around the province. Print copies are available in English or French from our office and the brochure can also be viewed and printed from our website.

Strengthening Sanctions for Intentional Privacy Violations

In our 2012 annual report, we reported on our investigation of a privacy breach where an employee of a trustee snooped in the electronic personal health information (PHI) of a patient to whom she was not providing care. This case highlighted that under PHIA it was not an offence for an employee to wilfully use or view PHI without legal authority under PHIA, such as by snooping – it was only an offence if the employee wilfully disclosed the PHI.

We also reported on proposed amendments to PHIA's offence provisions, introduced in the legislature in 2012, based on a recommendation we made after that investigation. We are pleased to note that the amendments received Royal Assent on December 5, 2013, making it now an offence for:

- an employee, officer or agent of a trustee, information manager or health research organization, to wilfully use, gain access to or attempt to gain access to another person's PHI without the authorization of the trustee, information manager or health research organization
- any person to knowingly falsify another person's PHI.

We recognize that most people who provide care to Manitobans also extend that care to their PHI. However, sanctions are essential because despite existing protections for PHI, there will be some people who intentionally flout the law. For example, it was reported in 2013 that in Saskatchewan, an employee of a regional health authority (RHA) abused her authorized access to an electronic health information system to view and change the personal health information of a co-worker who was also a patient of the RHA. The employee changed the PHI seven times, by replacing the patient's name with vulgarities, and by changing the patient's gender and infectious disease information.

In another case reported in 2011 in Alberta, a pharmacist had accessed drug information of members of her church congregation, via Alberta's provincial electronic health information system called Netcare (similar to eChart Manitoba). One of these members had complained to the church about the pharmacist's relationship with a male member of the congregation. The pharmacist then posted information on Facebook relating to prescription drugs being taken by the complainant and eight other women who the pharmacist believed were sympathetic to the complainant. Alberta's information and privacy commissioner referred the matter to the Alberta Department of Justice for prosecution and the pharmacist was charged with knowingly obtaining or attempting to obtain health information in contravention of the *Health Information Act*. She was fined $15,000.

There have been many other reported breaches across Canada, including several snooping breaches in Ontario hospitals and in one case reported in Newfoundland and Labrador in 2012, a nurse snooped in the records of 122 patients that were completely outside of her care. Although the nurse signed an oath of confidentiality, she stated that she felt justified in looking at these records because she claimed she wanted to help these patients, which included her ex-husband, her boyfriend's ex-wife, a friend who had a drug problem and someone who was renting an apartment from her.

These types of privacy violations have a traumatizing impact on the affected individuals, undermine trust in health-care providers and diminish public confidence in the health-care system. The new offence provisions in PHIA, with a penalty of up to $50,000 if convicted, should serve as a deterrent to those considering such activities and an appropriate consequence for such actions taken.

Sanctions for intentionally violating patient privacy are the last line of defense for protecting PHI. Robust privacy protection for PHI should include:

- creating a privacy respectful culture in the workplace that places a high value on protecting individuals' privacy and complying with PHIA
- promoting protection of PHI and preventing privacy breaches through implementing policies and safeguards and providing staff training about these
- ensuring staff are aware of the consequences for deliberate actions that violate PHIA and the privacy of individuals
- auditing to detect unauthorized activity such as snooping
- applying consequences, including sanctions such as the prosecution of offence, when deliberate privacy violations have occurred.

About the office

Manitoba Ombudsman is an independent office of the Legislative Assembly of Manitoba and is not part of any government department, board or agency. The office has a combined intake services team and two operational divisions – the Ombudsman Division and the Access and Privacy Division.

Under *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA), the Access and Privacy Division investigates complaints from people about any decision, act or failure to act relating to their requests for information from public bodies or trustees, and privacy concerns about the way their personal information or personal health information has been handled. "Public bodies" include provincial government departments and agencies, municipalities, regional health authorities, school divisions, universities and colleges. "Trustees" include public bodies and additional entities such as health professionals, medical clinics, laboratories and CancerCare Manitoba. Our office has additional powers and duties under FIPPA and PHIA, including auditing to monitor and ensure compliance with these acts, informing the public about the acts and commenting on the implication of proposed legislation, programs or practices of public bodies and trustees on access to information and privacy.

Under *The Ombudsman Act*, the Ombudsman Division investigates complaints from people who feel they have been treated unfairly by government, including provincial government departments, crown corporations, municipalities, and other government bodies such as regional health authorities, planning districts and conservation districts. The Ombudsman Division also investigates disclosures of wrongdoing under *The Public Interest Disclosure (Whistleblower Protection) Act* (PIDA). Under PIDA, a wrongdoing is a very serious act or omission that is an offence under another law, an act that creates a specific and substantial danger to the life, health, or safety of persons or the environment, or gross mismanagement, including the mismanagement of public funds or government property.

2013/14 Office Budget	
Total salaries and employee benefits for 32 positions	$2,737,000
Positions allocated by division are:	
Ombudsman Division 13	
Access and Privacy Division 8	
General 11	
Other expenditures	$519,000
Total Budget	**$3,256,000**

2013 Statistical Overview of the Office	
Intake and Administration	
Information or referrals provided by administration staff in response to inquiries	322
Inquiries and concerns handled by Intake Services	2104
Access and Privacy Division	
Complaints opened for investigation under *The Freedom of Information and Protection of Privacy Act* (FIPPA) (part 5)	210
Ombudsman-initiated reviews and investigations under *The Freedom of Information and Protection of Privacy Act* (part 4)	20
Complaints opened for investigation under *The Personal Health Information Act (PHIA)* (part 5)	25
Ombudsman-initiated reviews and investigations under *The Personal Health Information Act* (part 4)	5
Comments, consultations and collaborative initiatives under FIPPA and/or PHIA (part 4)	18
Ombudsman Division	
Complaints opened for investigation under *The Ombudsman Act*	66
Ombudsman-initiated investigations under *The Ombudsman Act*	9
Disclosures received under *The Public Interest Disclosure (Whistleblower Protection) Act* (PIDA)	47
Disclosures opened for investigation under PIDA	16
Child death review reports received under *The Child and Family Services Act*	68
Recommendations requiring follow-up	43
Inquest reports received under *The Fatality Inquiries Act*	2
Recommendations requiring follow-up	2

This chart shows the disposition of the 399 Access and Privacy cases investigated in 2013 under Parts 4 and 5 of FIPPA and PHIA

		Cases carried over into 2013	New cases in 2013	Total cases in 2013	Pending at 12/31/2013	Declined	Discontinued	Not Supported	Partly Supported	Supported	Resolved	Recommendations	Completed
Complaints opened for investigation under FIPPA (Part 5)													
Provincial Department	Aboriginal & Northern Affairs		5	5				1		4			
	Agriculture, Food & Rural Initiatives		2	2	1			1					
	Civil Service Commission		1	1				1					
	Conservation & Water Stewardship	2	7	9	2		1	2		3	1		
	Culture, Heritage & Tourism	1		1					1				
	Entrepreneurship, Training & Trade	2	5	7		1		5			1		
	Executive Council		1	1	1								
	Family Services & Labour	5	25	30	14		1	5	1	7	2		
	Finance		7	7	7								
	Health		4	4			1	3					
	Healthy Living, Seniors & Consumer Affairs	3	3	6	1			2		3			
	Housing & Community Development	1	1	2	2								
	Infrastructure & Transportation		3	3	2			1					
	Justice	2	7	9	2		1	4	1		1		
Crown Corporation & Government Agency	Automobile Injury Compensation Appeal Commission		1	1				1					
	Manitoba Agricultural Services Corporation	1		1							1		
	Manitoba Housing Authority	1	14	15	3	9		3					
	Manitoba Human Rights Commission		2	2	1			1					
	Manitoba Hydro	3	13	16	6		1	3		6			
	Manitoba Lotteries Corporation		1	1	1								
	Manitoba Public Insurance	1	8	9	2		1	6					
	The Funeral Board of Manitoba		1	1	1								
Local Government Body (LGB)	City of Brandon	3		3	2			1					
	City of Portage		1	1	1								
	City of Winnipeg	40	53	93	52	1	6	19	8	3	4		
	Town of Churchill		1	1					1				
	Town of Lac du Bonnet	1		1				1					
	Town of Ste. Anne	1	1	2				1	1				
	Town of The Pas		1	1				1					
	Town of Winkler		1	1					1				
	RM of De Salaberry		2	2						1	1		
	RM of Richot		1	1					1				
	RM of Rosser		2	2			1	1					
	RM of Siglunes		5	5	3		2						
	RM of Springfield	1	3	4				1		2	1		
	RM of Strathcona		1	1	1								
	RM of Victoria Beach	1	5	6	5			1					
	RM of Woodlands		1	1				1					
Educational Body (EB)	Louis Riel School Division		1	1				1					
	Mystery Lake School Division	1		1	1								
	Pembina Trails School Division		2	2	1				1				
	Red River College	5	1	6	2				4				
	River East Transcona School Division		1	1				1					
	St. James Assiniboia School Division		1	1	1								
	Winnipeg School Division	1		1				1					
	University of Manitoba	4	1	5				1	3		1		
	University of Winnipeg	2	2	4	1			1	1		1		
Health Care Body (HCB)	CancerCare Manitoba	1	5	6				3	3				
	St. Boniface General Hospital		3	3	1		1	1					
	Brandon Regional Health Authority	1		1	1								
	Prairie Mountain Regional Health Authority		1	1				1					
	Southern Regional Health Authority		2	2					2				
	Winnipeg Regional Health Authority	1	1	2				1			1		
Subtotal		**85**	**210**	**295**	**118**	**11**	**16**	**77**	**29**	**29**	**15**		
Complaints opened for investigation under PHIA (Part 5)													
Prov Dept	Entrepreneurship, Training & Trade		1	1						1			
	Family Services		2	2				1		1			
	Health		1	1	1								
Health Care Body	Diagnostic Services of Manitoba	1		1				1					
	CancerCare Manitoba	3		3	1						2		
	Medical Clinic		1	1							1		
	Health Sciences Centre		2	2				2					
	Personal Care Home		2	2				2					
	Interlake-Eastern Regional Health Authority		1	1						1			
	Brandon Regional Health Authority	1		1	1								
	Northern Regional Health Authority		1	1	1								
	Southern Regional Health Authority		2	2					2				
	Winnipeg Regional Health Authority	2	5	7				1		4	2		
LGB	City of Winnipeg		1	1	1								
EB	Pembina Trails School Division		1	1	1								
Gov Agency	Workers Compensation Board	1	1	2					1	1			
Health Prof	Physician		2	2			1				1		
	Physiotherapist		1	1	1								
	Psychologist		1	1	1								
Subtotal		**8**	**25**	**33**	**8**		**1**	**7**	**3**	**8**	**6**		

		Cases carried over into 2013	New cases in 2013	Total cases in 2013	Pending at 12/31/2013	Declined	Discontinued	Not Supported	Partly Supported	Supported	Resolved	Recommendations	Completed
Ombudsman-initiated reviews and investigations under FIPPA (Part 4)													
Provincial Department, Crown Corporation & Government Agency	Civil Service Commission		1	1	1								
	Conservation & Water Stewardship		1	1	1								
	Family Services		4	4	2			1					1
	Healthy Living, Seniors & Consumer Affairs		2	2	1								1
	Infrastructure & Transportation		2	2									2
	Justice	3	1	4									4
	Automobile Injury Compensation Appeal Commission		1	1	1								
	Manitoba Public Insurance		2	2	2								
Local Body	City of Winnipeg	2	3	5	2				2				1
	District of Pinawa		1	1	1								
EB	University of Manitoba		1	1	1								
HCB	Winipeg Regional Health Authority		1	1									1
Subtotal		**5**	**20**	**25**	**12**			**1**	**2**				**10**
Ombudsman-initiated reviews and investigations under PHIA (Part 4)													
Prov Dept	Family Services		1	1									1
	Health	1	1	2	1								1
Health Care Body	Interlake-Easten Regional Health Authority		2	2	1								1
	Prairie Mountain Regional Health Authority		1	1									1
	Southern Health Region	1		1									1
Subtotal		**2**	**5**	**7**	**2**								**5**
Comments, consultations and collaborative initiatives under FIPPA and PHIA (Part 4)													
	Public bodies, trustees and other	**21**	**18**	**39**	**19**								**20**
Total		**121**	**278**	**399**	**159**	**11**	**17**	**85**	**34**	**37**	**21**		**35**

Supported: Complaint fully supported because the decision was not compliant with the legislation.

Partly supported: Complaint partly supported because the decision was partly compliant with the legislation.

Not supported: Complaint not supported at all.

Recommendation made: All or part of complaint supported and recommendation made after informal procedures prove unsuccessful.

Resolved: Complaint is resolved informally before a finding is reached.

Discontinued: Investigation of complaint stopped by ombudsman or client.

Declined: Decision by ombudsman not to investigate complaint, usually based on a determination that the circumstances do not require investigation.

Completed: Cases conducted under Part 4 of FIPPA and PHIA where the task of auditing, monitoring, informing, or commenting has been concluded.

Pending: Complaint still under investigation as of January 1, 2014.

OPENED

Overview of Privacy Complaints Opened in 2013: 39 new complaints about privacy matters were opened under Part 5 of FIPPA and PHIA

Type of Privacy Complaint	FIPPA	PHIA	Total
Collection	4	-	4
Use	1	8	9
Disclosure	14	10	24
Security	-	2	2
Total	**19**	**20**	**39**

NA* Not applicable as requests cannot be disregarded under PHIA
NA** Not applicable as extensions cannot be taken under PHIA

Overview of Access Complaints Opened in 2013: 196 new complaints about access matters were opened under Part 5 of FIPPA and PHIA

Type of Access Complaint	FIPPA	PHIA	Total
Refused access	121	2	123
No response	25	1	26
Request was disregarded	1	NA*	1
Extension	6	NA**	6
Fees	9	-	9
Fee waiver	1	-	1
Correction	9	2	11
Third party contest	1	-	1
Other	18	-	18
Total	**191**	**5**	**196**

CLOSED

Overview of Access Complaints Closed in 2013: 169 complaints about access matters were closed under Part 5 of FIPPA and PHIA

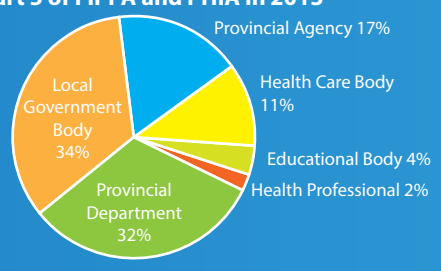
Type of Access Complaint	FIPPA	PHIA	Total	Declined or Discontinued	Supported in part or in whole	Not Supported	Resolved	Recommendation Made
Refused Access	105	2	107	10	27	55	15	-
No Response	18	1	19	3	14	1	1	-
Request was Disregarded	1	NA*	1	-	-	1	-	-
Fees	6	-	6	1	4	1	-	-
Fee Waiver	1	-	1	-	-	1	-	-
Correction	9	1	10	7	1	2	-	-
Extension	5	NA**	5	2	2	1	-	-
Other	20	-	20	4	3	10	3	-
Total	**165**	**4**	**169**	**27**	**51**	**72**	**19**	**-**

NA* Not applicable as requests cannot be disregarded under PHIA
NA** Not applicable as extensions cannot be taken under PHIA

Overview of Privacy Complaints Closed in 2013: 33 privacy complaints were closed under Part 5 of FIPPA and PHIA

Type of Privacy Complaint	FIPPA	PHIA	Total	Declined or Discontinued	Supported in part or in whole	Not Supported	Resolved	Recommendation Made
Collection	2	-	2	-	1	1	-	-
Use	2	10	12	-	7	3	2	-
Disclosure	8	9	17	1	8	8	-	-
Security	-	2	2	-	1	-	1	-
Total	**12**	**21**	**33**	**1**	**17**	**12**	**3**	**-**

Distribution of Complaints Opened Under Part 5 of FIPPA and PHIA in 2013



Types of Cases Opened in 2013