2016-2017 Annual Report

Navigating in a Digital World

Office of the
Saskatchewan Information
and Privacy Commissioner

Office of the
Saskatchewan Information
and Privacy Commissioner

503—1801 Hamilton Street
Regina SK S4P 4B4

Phone: 306-787-8350
Toll Free: 1-877-748-2298
Fax: 306-798-1603

Email: webmaster@oipc.sk.ca
Website: www.oipc.sk.ca
Twitter: @SaskIPC

Office of the
Saskatchewan Information
and Privacy Commissioner

June 20, 2017

Hon. Corey Tochor
Speaker of the Legislative Assembly
129 Legislative Building
Regina, Saskatchewan
S4S 0B3

Dear Mr. Speaker:

I have the honour to present my third Annual Report as Information and Privacy Commissioner for Saskatchewan. I have prepared this Annual Report in accordance with the provisions of subsection 62(1) of *The Freedom of Information and Protection of Privacy Act*, subsection 52(1) of *The Local Authority Freedom of Information and Protection of Privacy Act* and subsection 60(1) of *The Health Information Protection Act*.

I thank the Members of the Legislative Assembly for their support of the Office of the Information and Privacy Commissioner and I ask for their cooperation in changing legislation to recognize that we live in a digital world.

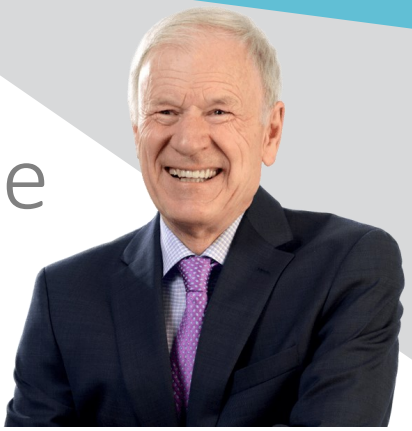
I also thank the staff of the office for their hard work over the last year in accomplishing some ambitious goals and developing a new three year plan.

Respectfully submitted,

Ronald J. Kruzeniski, Q.C.
Information and Privacy Commissioner

Table of Contents

Commissioner's Message



I was appointed Commissioner in July of 2014 and began my term focusing on five key core areas. These included: Citizens First, A New Look, Information for All, Updating the Rules and being Efficient and Effective. This past year my office has made great progress in each of these areas.

Our focus over the last three years has been to provide citizens and public bodies with our reports or responses sooner. Our priority in the next 3 years will still be to provide applicants and organizations reports and responses as soon as we can. Because we had made significant progress in the 5 year plan, it was decided it was time to develop a new plan. In the following pages I will report on our achievements under the old plan but also outline our objectives under our new 3 year plan.

In my 2015 Annual Report, I said it is time to update *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). These statutes had not been updated in 25 years and 24 years respectively. I made recommendations for change. The Legislative Assembly on May 18, 2017 gave third reading to Bill 30, *The Freedom of Information and Protection of Privacy Amendment Act, 2016* and Bill 31, *The Local Authority Freedom of Information and Protection of Privacy Amendment Act, 2016*. I look forward to the proclamation of these two Bills and the implementation of the updated provisions.

In my 2016 Annual Report, I made proposals to amend *The Health Information Protection Act* (HIPA). A summary of those proposed amendments can be found at www.oipc.sk.ca. I look forward to working with the Minister of Health and officials in the Ministry of Health to move those proposals to the next stage in the legislative process.

The office intervened in a case at the Supreme Court of Canada where an issue was being argued as to the extent of solicitor-client privilege. This case may have significant implications for Saskatchewan for solicitor-client privilege in Canada. My office initiated an application in the Court of Queen's Bench where the University of Saskatchewan claims solicitor-client privilege. The decision has been released and can be found at www.oipc.sk.ca under the Legislation tab (this decision has been appealed to the Saskatchewan Court of Appeal).

This year my office embarked upon a project to redesign and redevelop its website. The aim is to make the office's website the primary means of communicating with citizens, public bodies, health trustees and elected officials. You can view our new website at www.oipc.sk.ca.

In closing, I want to express my appreciation to the staff of the office for their hard work, dedication and commitment to ensuring access and privacy rights are afforded to the citizens of Saskatchewan. I also want to thank our many stakeholders including applicants, complainants, public bodies, and health trustees for their continued cooperation with our office.

I am looking forward to my fourth year as Commissioner and embarking upon accomplishing the new 3 year plan.

Ronald J. Kruzeniski, Q.C.
Information and Privacy Commissioner

About Us

Our Mandate

The Office of the Saskatchewan Information and Privacy Commissioner (IPC) is an independent office of the Saskatchewan Legislative Assembly. It oversees three Saskatchewan statutes: *The Freedom of Information and Protection of Privacy Act* (FOIP); *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP); and *The Health Information Protection Act* (HIPA).

FOIP, LA FOIP and HIPA establish the access to information and privacy rights of citizens.

The IPC ensures that public bodies respect the privacy and access rights of the citizens of Saskatchewan by:

- informing members of the public of their information rights;
- resolving access and privacy disputes between individuals and public bodies;
- making recommendations on appeals from access to information decisions by public bodies;
- investigating and resolving privacy complaints;
- issuing recommendations on public bodies' policies and practices; and
- commenting on proposed laws and policies.

Our Mission

To ensure that access to information and privacy rights in Saskatchewan are respected.

Accomplishments 2016-2017

Citizens First

Goals

- Establish and reach a goal that citizens and public bodies will receive their report, response or a resolution within 33 days, 80% of the time.
- Support the Ministry of Justice in a project to replace the Privacy Framework 2003.
- Develop a best practices document on the creation, storage and destruction of text messages.

Accomplishments

- In the third quarter of the fiscal year the office achieved a result of 35 days, 80% of the time but because of an increased workload the response time increased to 47 days, 80% of the time.
- The Ministry of Justice continues to work on replacing the Privacy Framework 2003 with a new set of tools.
- Work has begun but is not yet completed.

A New Look

Goals

- Re-design and re-platform the office's website.

Accomplishments

- Re-design completed. New website operating at fiscal year end.

Information for All

Goals

- Participate in finalizing a joint project with the Ministry of Justice and the Public Service Commission (PSC) to complete four training modules on privacy and access for public servants.
- Promote a joint project with the Ministry of Justice and PSC to develop an annual refresher access and privacy online course for public servants.
- Promote and participate in a project with the Ministry of Justice and the PSC to take the four PSC modules and convert them to LA FOIP terminology and make them available to local authorities.
- Promote a joint project with the Ministry of Health and PSC to develop a training module on HIPA for public servants.
- Finalize and publish the *IPC Guide to HIPA* for trustees.
- Develop resources for Medical Residents and their duties under *HIPA.*
- Promote and participate in a joint project with eHealth Saskatchewan on developing auditing guidelines for trustees.
- Continue to update, develop and expand the *IPC Guide to Exemptions* for FOIP and LAFOIP and post to the website.
- Develop a guidance document regarding best practices for Arbitrators.
- Develop and present a workshop for severing in the paper and electronic world.

Accomplishments

- The content of the modules is complete and it is expected the modules will be released in the coming months.
- The four modules referred to above can be used for this purpose. My office continues to promote the need for public servants to have an annual refresher.
- This project will be started after the four FOIP modules have been released.
- This office has promoted such a training module.
- The *IPC Guide to HIPA* is complete and available on our website.
- This resource is completed and on our website.
- The auditing guidelines are completed and posted on eHealth's website and IPC website.
- The *IPC Guide to Exemptions* is updated and posted to our website.
- A guide was developed for Arbitrators and posted on our website.
- Work has begun on a webinar.

• Promote and participate in discussions with the Saskatchewan Medical Association (SMA) to ensure their and IPC resources are complementary to one another	• Consultations with the SMA occurred.
• Update/develop guidelines for tribunals in publishing their decisions.	• A guide was developed for Tribunals and posted on our website.
• Develop guidelines on when to get consent from mature minors and post to the website.	• A resource was developed and posted to our website.
• Promote and participate in a joint project to develop an online module for staff of the Saskatchewan Cancer Agency and other trustees and their staff.	• This office promoted the development of an online module.

Updating the Rules

Goals

- Implement changes as a result of proposed amendments to Bill 30, *The Freedom of Information and Protection of Privacy Amendment Act, 2016* and Bill 31, *The Local Authority Freedom of Information and Protection of Privacy Amendment Act, 2016*.
- Propose and promote amendments to the *HIPA* Regulations.
- Begin the work of developing *Personal Information Protection* legislation for Saskatchewan.
- Research and develop a position or guideline document for professionals regarding transparency on the discipline of members.
- Promote and participate in a joint project where executive government, crown corporations, health regions, trustees and municipalities develop an online individual authentication system with adequate privacy protection.

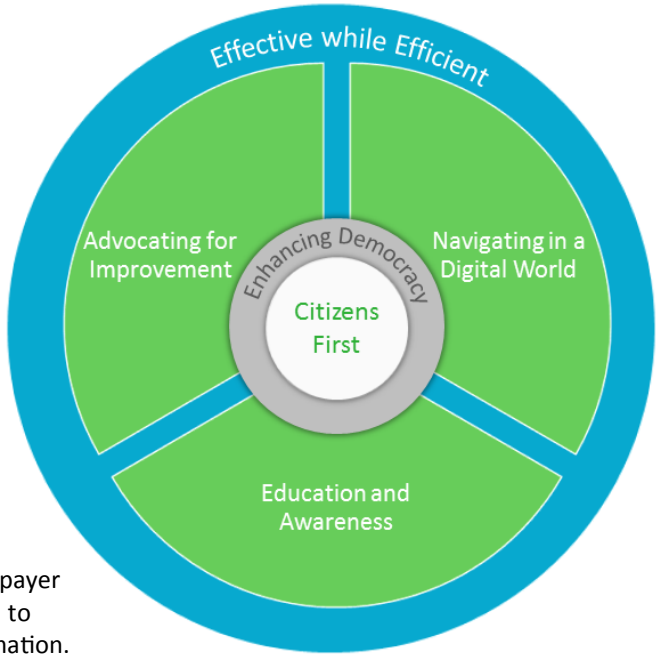
Accomplishments

- Royal assent was given and we are now awaiting proclamation of the Bills.
- Proposals have been made to the Ministry of Health.
- Work on this will continue in 2017-2018.
- A guide was developed for self-governing discipline bodies and posted on our website.
- This office has promoted the development of an online individual authentication system.

Plan for 2017-2018

Citizens First

- Core to our work is that we support access to records as requested by citizens in a timely manner and promote protection of the privacy of those citizens wherever required. All other objectives in this document are intended to enhance and protect the rights of citizens to obtain information.



Enhancing Democracy

- The freedom of information legislation in the province enshrines the principle that citizens should have access to information generated by organizations supported by tax payer dollars. All other objectives in this document are intended to enhance and protect the rights of citizens to obtain information.

Education and Awareness

- Visit every police force in the province to discuss the amendments to LA FOIP.
- Develop informational awareness packages that could be forwarded to all police forces that are new to LA FOIP.
- Promote within the government of Saskatchewan that every new employee and every employee annually take the four training modules on privacy and access for public servants.
- Develop and post to the website the IPC Rules of Procedure.
- Develop and post a guideline on the treatment of non-responsive records or information.

Navigating in a Digital World

- Promote and work with the Ministry of Central Services to develop a new approach and system for the retention, and archiving of emails where retrieval is possible at a low cost in government.
- Do a study as to whether using the Cloud housed in Canada is more secure than local storage.
- Promote and encourage a joint project where executive government, crown corporations, and the provincial health authorities, develop an online individual authentication system with adequate privacy protection.

Advocating for Improvement

- Develop policies, practices and guidelines as a result of amendments to FOIP and LA FOIP.
- Develop proposals for amendments to FOIP and LAFOIP Regulations.
- Promote amendments to update HIPA and work with the Ministry of Health to develop proposed legislation.
- Develop proposals to create a *Personal Information Protection Act* in Saskatchewan or amendments to *The Saskatchewan Employment Act*.
- Promote *HIPA Regulation* amendments to broaden the definition of trustee, allow reporting of crimes by trustees and trainees' access to PHI.
- Promote a study to update the model *Professions Act.*
- Propose further amendments to FOIP and LAFOIP and work with the Ministry of Justice to develop proposed legislation.
- Promote stand-alone Act on data matching and work with the Ministry of Justice to develop proposed legislation.
- Promote amendments to the Workers' Compensation Act and work with the Workers' Compensation Board and the Ministry of Justice to develop proposed legislation.

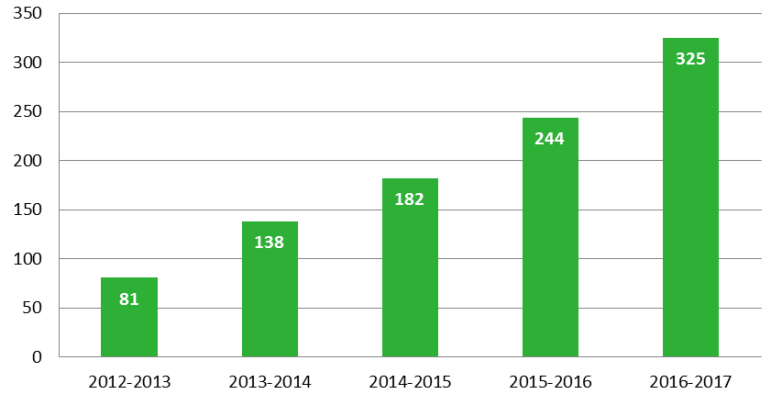
Effective While Efficient

- Issue a Notification letter or resolve a matter within 6 days, 80% of the time.
- Issue a Report or resolve a matter on review of an access request within 75 days, 80% of the time.
- Issue a Report or resolve a matter regarding breach of privacy within 65 days, 80% of the time.
- Complete or close Consultation files within 10 days, 80% of the time.
- Develop a database to track the provision of summary advice by the office.
- Conduct the second privacy awareness survey in March 2018.
- Explore the feasibility of a case records management system.

Files and Reports

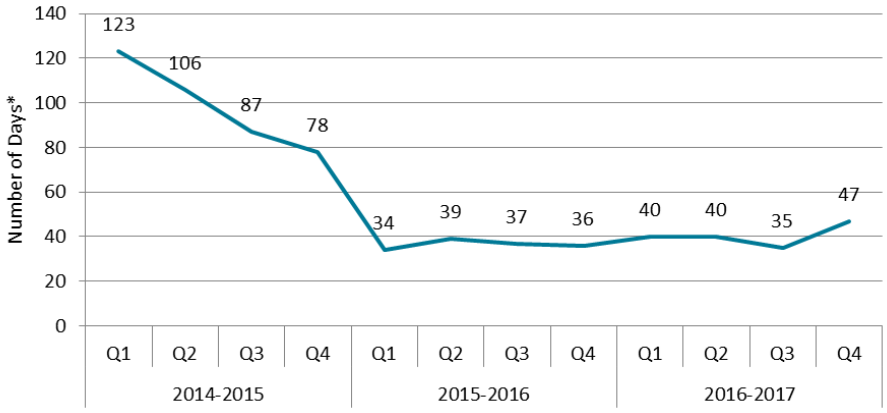
Increase in Files

The office is experiencing a notable increase in reviews, investigations and consultations, resulting in more files being opened as is reflected in the Bar Chart below. This resulted in a 37% increase over the previous year.



Increase in Response Time

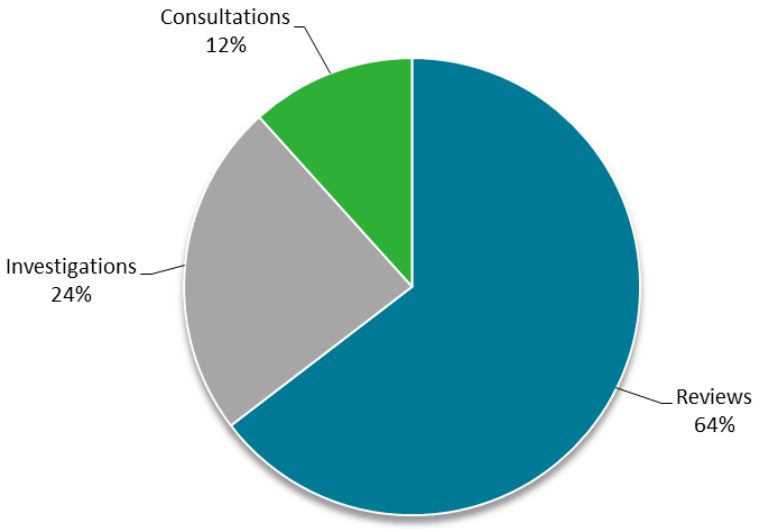
The office has worked hard to improve its response time to citizens and public bodies. In 2016-2017 year, the response time increased mainly due to a 37% increase in files opened.



*Number of days that citizens and public bodies received their report, response or a resolution, 80% of the time.

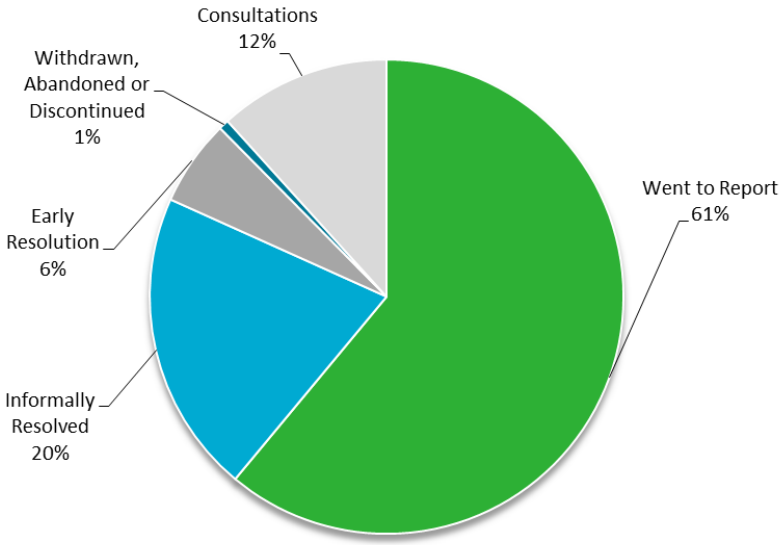
Types of Files Opened

The office opened 325 files in the 2016-2017 fiscal year. This is a chart summarizing the types of files opened.



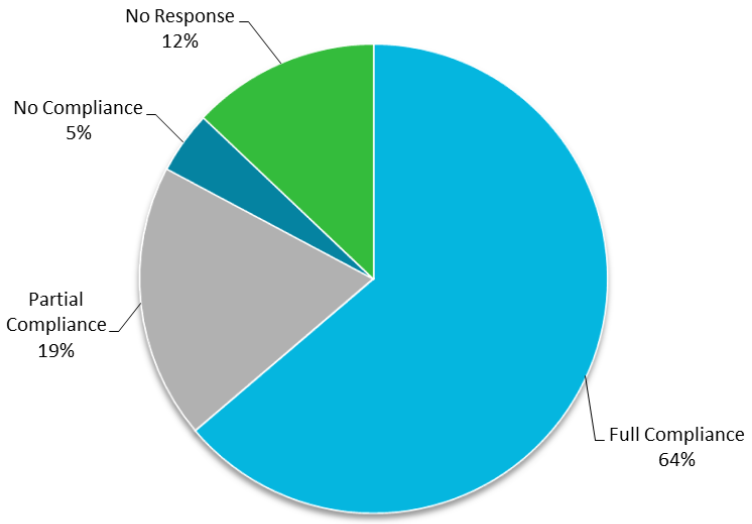
Resolution of Files

The office closed 290 files in the 2016-2017 fiscal year. This is a chart summarizing the percentages of files resolved in different ways including issuance of a Report.



Compliance with Recommendations

The office issued 117 Reports in 2016-2017. A public body or trustee is required to respond to the recommendations within 30 days of receiving the Report. Below is a chart showing the percentage of Reports where there is full compliance, partial compliance and no compliance.



My office is obligated to report on the recommendations that were not complied with. See *The Freedom of Information and Protection of Privacy Act,* subsection 62(2), *The Local Authority Freedom of Information and Protection of Privacy Act* subsection 52(2) and *The Health Information Protection Act* subsection 60(2).

Failure to respond to a report is considered to be non-compliance. On the following pages are three tables. The first table lists those public bodies that responded to a Report with partial compliance. The second table lists those public bodies that responded to a Report with no compliance. The third table lists those public bodies that did not respond at all.

Partial Compliance

Government Institution	Report #	Recommendation(s) not complied with*
Global Transportation Hub	Review Report 157-2016	[65]
Global Transportation Hub	Review Report 158-2016	[62]
Global Transportation Hub	Review Report 159-2016	[90]
Ministry of the Economy	Review Report 277-2016	[82]
Ministry of the Economy	Review Report 302-2016	[67]
Ministry of Environment	Review Report 116-2016	[27]
Ministry of Finance	Review Report 165-2016	[22]
Ministry of Government Relations	Review Report 178-2016	[32]
Ministry of Health	Review Report 016-2016	[72]
Ministry of Justice	Review Report 027-2016	[68], [69]
Saskatchewan Government Insurance	Investigation Report 189-2016	[46], [51]
Local Authority	**Report #**	**Recommendation(s) not complied with***
Saskatchewan Polytechnic	Review Report 273-2016	[52]
Town of Kindersley	Review Report 147-2016	[26], [27]
Town of Kindersley	Review Report 149-2016	[25]
Town of Kindersley	Review Report 151-2016	[45]
Town of Kindersley	Review Report 152-2016	[23], [25]
Town of Kindersley	Review Report 153-2016	[24]
Town of Kindersley	Review Report 154-2016	[23]
University of Saskatchewan	Review Report 153-2015	[83]
University of Saskatchewan	Review Report 164-2016	[30]
Trustee	**Report #**	**Recommendation(s) not complied with***
Prince Albert Parkland Regional Health Authority	Investigation Report 170-2016	[56], [57]
Regina Qu'Appelle Regional Health Authority	Review Report 214-2015	[49]

***refers to paragraph # in the Report. Click on the link to go directly to the Report.**

No Compliance

Government Institution	Report #	Recommendation(s) not complied with*
Ministry of the Economy	Review Report 223-2016	[43]
Ministry of Highways and Infrastructure	Review Report 191-2016	[21]
Ministry of Highways and Infrastructure	Review Report 306-2016	[29], [30]
Saskatchewan Government Insurance	Review Report 229-2015	[48]
Saskatchewan Government Insurance	Review Report 054-2016	[26], [27]
Local Authority	**Report #**	**Recommendation(s) not complied with***
R. M. of Rosthern	Investigation Report 237-2016	[28], [29], [30], [31], [32]

***refers to paragraph # in the Report. Click on the link to go directly to the Report.**

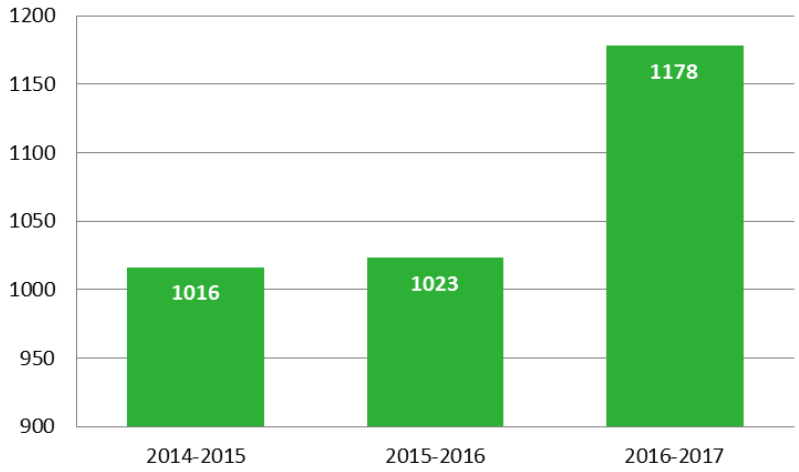
No Response Received

Government Institution	Report #	Recommendation(s) not complied with*
Ministry of Highways and Infrastructure	Review Report 064-2016 to 076-2016	[55], [56]
Ministry of Highways and Infrastructure	Review Report 123-2016 to 135-2016	[19]
SaskPower	Investigation Report 120-2016	[37]
Local Authority	**Report #**	**Recommendation(s) not complied with***
Northern Village of Pinehouse	Review Report 036-2016	[22]
Northern Village of Pinehouse	Review Report 039-2016	[20], [21]
Northern Village of Pinehouse	Review Report 056-2016	[17], [18]
Northern Village of Pinehouse	Review Report 098-2016	[31], [32], [33]
Northern Village of Pinehouse	Review Report 106-2016	[9]
Northern Village of Pinehouse	Review Report 110-2016	[17], [18], [19]
Northern Village of Pinehouse	Review Report 171-2016	[11]
Trustee	**Report #**	**Recommendation(s) not complied with***
Heartland Regional Health Authority	Review Report 121-2016	[26]
Saskatchewan Registered Nurses' Association	Investigation Report 109-2016	[49], [50]

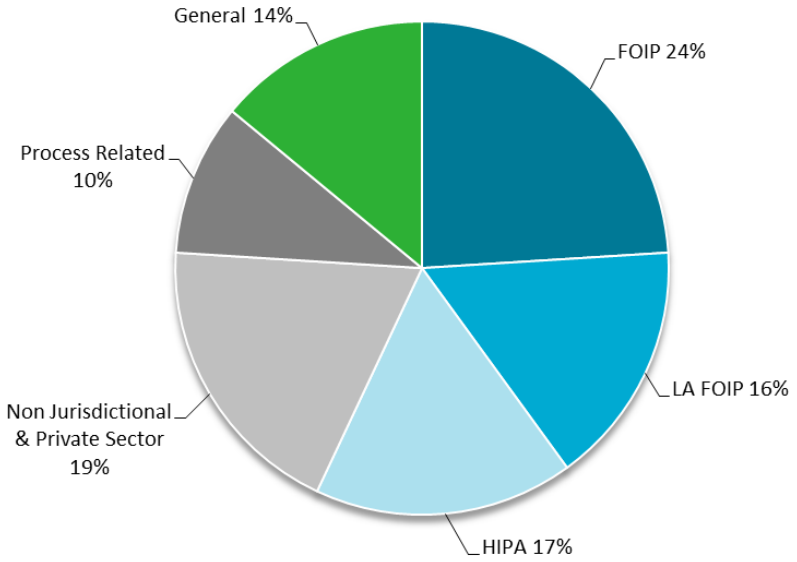
***refers to paragraph # in the Report. Click on the link to go directly to the Report.**

Increase in Requests for Advice

The mandate of the office is to provide education and a good portion of that education takes the form of people contacting the office and obtaining advice. In 2016-2017 the office provided summary advice on nearly 1200 occasions. This is a 15% increase over 2015-2016.



From the chart below, it is clear that the office gives advice related to the three main statutes where the office has jurisdiction. Nearly 60% of summary advice was given related to these pieces of legislation.



Navigating in a Digital World

There is no doubt that we are living in a digital world. Our newspapers and news channels are filled with stories about electronic access, breaches, snooping and privacy. Organizations are shifting from storing information on paper, to storing it electronically. Organizations and people within them communicate by email, text and webinars. We register for things and order things online and in the process provide a lot of personal information and personal health information. Below I raise just a few issues that will face us in the digital world that we live in.

Data Matching

My office has issued a document regarding data matching in the province of Saskatchewan. That paper outlines the meaning of the word, the benefits, the risks, a review of legislation in other countries and provinces, the inadequacies of current Saskatchewan legislation and the needs in the Saskatchewan environment. This report can be found at https://oipc.sk.ca/assets/data-matching.pdf.

I am recommending a stand alone piece of legislation based on the following principles and containing the following elements.

Any legislation in Saskatchewan should embrace the principles outlined below.

1. Establishing Purpose
Government institutions, eHealth Saskatchewan and the provincial health authority should be able to clearly state the purpose of each data matching project prior to performing any data matching.

2. Data Minimization
The least amount of identifiable information should be used for data matching projects.

3. De-identification
When designing a data matching project, government institutions, eHealth Saskatchewan and the provincial health authority should consider if the purpose of a data matching project can be achieved using de-identified information. If so, then only de-identified information should be used.

4. Accuracy
Government institutions, eHealth Saskatchewan and the provincial health authority should only use carefully selected data sets that contains accurate, complete, and up-to-date information to avoid generating biased or discriminatory results.

5. Openness
Government institutions, eHealth Saskatchewan and the provincial health authority should notify the individuals whose personal information is being used in a data matching project. They should also notify these individuals about any personal information that is being generated about them. Individuals should be able to gain access to their own personal information upon request.

6. Establishing Safeguards
Government institutions, eHealth Saskatchewan and the provincial health authority should establish physical, administrative, and technology safeguards to prevent unauthorized access to personal information that is collected, used, disclosed, or generated in a data matching project.

As a result, I recommend the government of Saskatchewan propose and the Legislative Assembly consider a stand-alone Act dealing with data matching which would have the following elements:

- A definition of data matching.
- Prohibition of data matching unless in accordance with the Act.
- Limiting data matching to government institutions, eHealth Saskatchewan and the provincial health authority.
- Requirements before starting a data matching project, including: 1) privacy impact assessment, 2) the definition of purpose and scope, 3) documenting in an agreement and 4) notifying the Commissioner of each project.
- Require destruction of data generated.
- Require information about data matching projects to be posted on website.
- Allow citizens to find out whether they are part of the data matching project.
- Require a report after a data matching project is complete.

Email Storage

As public bodies have gone to doing the majority of their communicating by email, access requests for records of emails have increased. I expect such requests will continue. If the access request is for recent records (emails) an employee can perform a search in Outlook (or other email program) and very quickly locate the emails related to the access request. If the requests are for older emails, which have been archived in the Outlook archive system, the search can still be done (it might take a little longer). If the access request is for emails that are no longer in the Outlook system, then the search might be more difficult depending on the technology used. Or, if the employee has left the organization, and his or her emails have been stored outside the Outlook system, the effort to get those emails could be difficult and time consuming. This can be hard work or expensive to find the relevant records.

The best solution is that emails be reviewed regularly by each employee and the ones that are part of the official public record, get stored in an organized electronic filing system, such as a shared drive that is accessible to authorized employees or an electronic document records management system. I can assure you, this does not always happen but it should. The next best solution is that an organization acquires an email management system that stores all emails old and new for current and former employees.

The least desirable but still acceptable method of managing email is to print and file official records. Out of the three solutions, I encourage public bodies to adopt the first but failing that implement the second.

Posting to the Web

My office has always and will probably always, encourage public bodies to be open and transparent. The phrase can mean different things to different people. Some organizations are moving towards being more open. One way is for them to publish on their website information released in an access request. This is a positive step in that it provides more information to the public and hopefully saves the organization time in handling similar or repetitive access requests. There is a limit here in that the organization cannot and should not release my or your personal information or third party confidential information in the process.

Another dimension to this issue is decision making bodies publishing their decisions. Whether they are a tribunal, arbitrator or discipline committee of a professional body, they need to strive towards openness. At the same time they need to strike a balance in terms of the amount of personal information that is released. Posting a decision to a website is like publishing to the entire world. Billions of people have access to what is posted on our websites. There is a need to post decisions but there is also a need to de-identify those decisions as much as is reasonable and practical. I would encourage every public body and every decision maker to carefully review its policy and practices when it issues a decision and then publishes it on the web. We need to keep in mind that posting to the web probably means the decision will be available forever.

Breaches from the Inside

My office receives many reports regarding employees or those with access snooping into databases. Such snooping is a breach of privacy and those employees who do it should be appropriately disciplined. Many organizations have policies prohibiting an employee from looking up his or her own or family personal information.

There is another side to employee conduct that is worrisome. Security experts will say that breaches from the outside are often caused by an employee doing something careless on the inside. One of the most common is an employee clicking an attachment or a link in an email that results in an outsider being able to install a program on the employees' computer that allows access or future access. All employees everywhere need to exercise abundant caution and not open unfamiliar emails, suspicious attachments or links. Recent events in the world reinforce the need for employee caution and virulence. Recent events reinforce the need for annual employee refresher training on access and privacy.

Hacking from the Outside

Recent events make it clear that hackers anywhere in the world may have an interest in reaching an organization's computer system. They are becoming more sophisticated. Through things like ransomware or identity theft, they have found a way to make money. We all need to become more conscious of threats from phishing, hacking and malware, including ransomware.

System administrators in the world, in our country and in our province need to protect all of us, all the time. Patches need to be installed immediately. We need to be using the most up- to-date versions of programs and

systems. Monitoring efforts need to continue to increase. This will cost money but the failure to do so may cost a lot more.

I encourage decision makers to support system administrators with funds and resources to safeguard our networks and databases and reduce the risk of external attacks. It would appear this will be a never-ending, relentless struggle. As the hackers are blocked in one direction, they will find another, and another and another.

Facial Recognition

As I read many articles and organizational announcements, facial recognition is here and a tool that will be used more often by organizations. As time goes on, the number of faces that are in the databases will obviously grow. As organizations see facial recognition as more effective, they will want to use it for their purposes which they will define as good purposes that benefit society. As a society, we will need to decide to what extent we will allow organizations to use this technology. Our face is part of our personal information. In some instances, we may choose not to agree to our picture being taken. As the technology evolves, it may be harder for us to refuse as we won't get the benefit we want without agreeing to our picture being taken. There are other instances where we won't even know that our picture has been taken. Finally with the millions of smart phones with cameras, any passerby could take our picture without us ever knowing. I expect we will be discussing this issue in the years to come, in our province.

Mobile Devices

We are quickly coming to the situation where everyone carries a smart phone, maybe two of them and a tablet too. It is necessary to distinguish between personal devices and devices paid for by a public body with tax payer dollars. A personal device is one owned and paid for by an employee. It is not appropriate to be used for work, in other words to carry on the business of the public body. Each public body should have or develop a policy regarding use of personal devices for work and in the workplace.

A mobile device owned or paid for by a public body will obviously have work related emails, text or images. Some of those emails, text or images will be part of the official record of that public body and public bodies need to have procedures in place to capture and store those items they determine as part of their official record. The Provincial Archives of Saskatchewan has developed a document entitled "Email Management Guidelines" which can be found at http://www.saskarchives.com/sites/default/files/pdf/fin.pdf.

Employees can have their office emails forwarded to their work phone. They can text one another regarding work issues. They can take a picture of a situation, another employee, a customer, client or patient. In these ways they are ending up with personal information on their mobile device.

Emails forwarded to their work phone may involve work information including personal information and personal health information. If the work phone is lost, someone might unlock it and access the work information. At home, do they let their children use or play games on their work phone? Does their spouse or partner have access to the work phone?

Regarding texts, if they involve important decisions, does the employee ensure those texts get on the official file? Do most texts just get deleted?

Regarding pictures, who else besides the employee, get to see those pictures? Does the employee send the pictures to other employees, family members or other professional colleagues? Does he or she post some of those pictures on a social media website which is accessible by friends, family or the public?

As you can see, our prized possession, our smart phone (personal or work), and our desire to take them everywhere, raises a lot of questions. Public bodies need to be clear as to what staff can and cannot do with their smart phone. Failure to have strong policies and enforcement runs the risk of privacy breaches.

The Cloud

When service providers began offering storage of our data in the cloud, we in Canada became nervous partly because of the Patriot Act (now the Freedom Act) and partly because of the level of security. Service providers have begun offering cloud services housed on servers in Canada. This takes away the U.S. legislation issue. The other concern is security. With recent events, it is hard to know what server or what database is truly safe. The service providers of cloud services will present the argument that they can provide greater security than one has now (and at lower cost). All of us will need to determine whether that is in fact true. I expect there will be greater discussion on the pros and cons of the cloud in the years and months ahead.

Any organization that is considering the cloud should ask some of the following questions and ensure they reduce risks by having their concerns documented in the service agreement.

What assurances do you have that your data is segregated from others? How do you know for certain that the cloud provider is not using your data for its own purposes? Can you audit/inspect to test the providers' compliance with agreements? It is hard to do if they are far, far away. What happens with your data upon termination of the agreement?

The Provincial Archives of Saskatchewan has issued a document entitled "Cloud Computing and Records Management" which can be found at http://www.saskarchives.com/sites/default/files/pdf/cloud_computing_fin_oct2016.pdf.

Cost of Protection

We as a society have enjoyed many benefits in our electronic digital age. We enjoy our smart phones and tablets and appreciate the portability of these devices. Our legislation existing and to be proclaimed, imposes upon public bodies and those who provide service to public bodies, a duty to protect personal information and personal health information. From the stories around the world, the breaches, the damage to reputation and the costs to remedy a breach, there is no doubt that public bodies will be required to spend much more to safeguard the information they have collected from their citizens.

In conclusion, welcome to our digital world. We all enjoy the benefits of that world and all of us must strive to reduce the risks of our personal information and personal health information getting into the wrong hands.