Office of the
Saskatchewan Information
and Privacy Commissioner

ANNUAL REPORT 2017-2018

Reducing the Risks

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 19, 2018

Hon. Mark Docherty
Speaker of the Legislative Assembly
129 Legislative Building
Regina, Saskatchewan
S4S 0B3

Dear Mr. Speaker:

I am pleased to present my fourth 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 continuing to implement a new three-year plan. My office has also been faced with increased requests for reviews or investigations, which continue to put pressure on the office to get reports out in a timely manner.

Respectfully submitted,

[redacted]

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

Table of Contents

Commissioner's Message

My office introduced a new three year plan in last year's Annual Report and in this Report I will report on our progress.

In my 2014-2015 Annual Report I said, "It's 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 significantly updated since their introduction in 1992 and 1993 respectively. I made recommendations for change. The Legislative Assembly, in the spring of 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*. These Acts were proclaimed effective January 1, 2018. My office has been, and continues to be, very involved in implementing and informing citizens and public bodies of the new provisions.

In my 2015-2016 Annual Report, "Striking a Balance", 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. Those amendments to HIPA have not materialized yet and I look forward to working with the Minister of Health and officials in the Ministry on those proposals and moving to the next stage in the legislative process.

In my Annual Report for 2016-2017, I addressed the issues relating to "Navigating in a Digital World". So much of what we do today is now electronic and my office and society need to continue to adjust its approaches to access and privacy in this digital world.

In this year's Report, "Reducing the Risks", I want to focus further on how, in our digital world, organizations may reduce the risk of privacy breaches. Breaches can occur with paper files but all of the noteworthy breaches today involve electronic files and can impact thousands of people.

My office initiated an application in the Court of Queen's Bench where the University of Saskatchewan claimed solicitor-client privilege. The Court of Queen's Bench decision was appealed to the Saskatchewan Court of Appeal. The Court of Appeal's decision was issued on May 16, 2018 and can be found at www.oipc.sk.ca.

This year, my office embarked upon a project to redesign and redevelop its case file management system and the new system was implemented in the spring of 2018. The new system will make my office more efficient in tracking the increased file load and safeguarding the storage of relevant documents and communications.

In last year's Report, I reported on a new website design. My office continues to improve the website and make it our primary source of communication with citizens, public bodies and elected officials. You can view our website at www.oipc.sk.ca.

I am looking forward to my fifth year as Commissioner and continuing to implement the new three-year plan. In addition to implementing our plan, my office will be hosting the National Information and Privacy Commissioners Conference in Regina in September 2018.

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.

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, policies and practices.

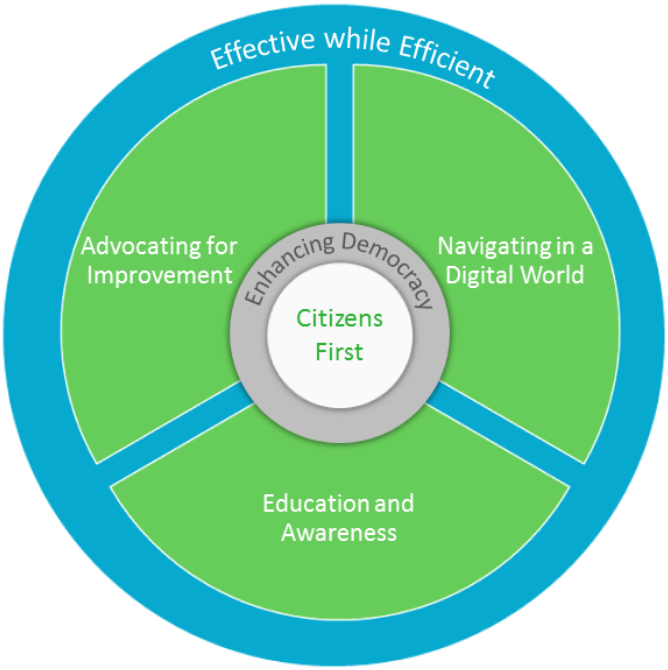
Our Mission

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

Accomplishments 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 taxpayer dollars. All other objectives in this document are intended to enhance and protect the rights of citizens to obtain information.

Education and Awareness

Goals	Accomplishments
Visit every police force in the province to discuss the amendments to LA FOIP.	I have met with the Saskatchewan Police Chiefs Association and am willing to work on joint training in the coming year. My office is working with the privacy coordinators in individual police forces as requested.
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.	In all reports and presentations, annual mandatory privacy training is recommended as the best practice.
Develop and post to the website *The Rules of Procedure*.	A draft copy of *The Rules of Procedure* has been posted and will be made final in the Spring of 2018.

Goals	Accomplishments
Develop and post a guideline on the treatment of non responsive records or information.	Prepared and posted a blog on non-responsive records (see *What about the non-responsive record?*).
Develop and post a dictionary of access and privacy terms.	The *Dictionary* was developed and was posted to the website in April 2018.
Develop and post a best practices document on the creation, storage and destruction of text messages.	A guide was developed and posted to our website in the spring of 2018 (see *Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools*).
Develop and conduct a webinar question and answer period for RMs.	Developed a webinar entitled *LA FOIP Sound Bytes – Q&A Webinars for Cities, Towns, Villages, Rural Municipalities, etc.*
Develop and post guidelines on the collection, use, storage and disclosure of the results of genetic tests.	A blog was posted on our website (see *Guidelines for the use of genetic information*).
Develop and post guidelines for the protection of personal health information in the reception room/ emergency/common areas of health care professionals' facilities.	A blog was posted on our website (see *Wait! Protect that phi in your waiting room!*).
Acquire a booth and make presentations at the SARM, SUMA and UMAAS Conventions.	Made a presentation and had a booth at the SUMA Convention.

Navigating in a Digital World

Goals	Accomplishments
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.	Promoted a new system for the retention and archiving of emails. Central Services is proceeding in that direction. The office has begun a study on backup tapes which relates in part to the storage of emails.
Do a study as to whether using the Cloud housed in Canada is more secure then local storage.	Organized presentations from Microsoft regarding security in the Cloud.

Advocating for Improvement

Goals	Accomplishments
Develop policies, practices and guidelines as a result of amendments to FOIP and LA FOIP.	A major effort was undertaken to update resources relating to the new amendments and best practices. These resources can be viewed at www.oipc.sk.ca.
Develop proposals for amendments to FOIP Regulations and LA FOIP Regulations.	Proposals were provided to the Ministry of Justice. FOIP and LA FOIP amendment regulations took effect on January 1, 2018.
Promote amendments to update HIPA and work with the Ministry of Health to develop proposed legislation.	No progress.
Develop proposals to create a *Personal Information Protection Act* in Saskatchewan or amendments to *The Saskatchewan Employment Act*.	No progress.
Promote HIPA Regulations amendments to broaden the definition of trustee, allow reporting of crimes by trustees and trainees' access to personal health information.	The office continues to promote HIPA Regulations amendments.
Propose further amendments to FOIP and LA FOIP and work with the Ministry of Justice to develop proposed legislation.	The office is working on the amendments that came into force January 1, 2018 and will, in the next number of years, propose other amendments to FOIP and LA FOIP.
Promote a stand-alone Act on data matching and work with the Ministry of Justice to develop proposed legislation.	*The Data Matching Agreements Act* received royal assent.
Promote amendments to *The Workers' Compensation Act, 2013* and work with the Saskatchewan Workers' Compensation Board to develop proposed legislation.	My office and the Board have agreed to amendments.

Effective While Efficient

Goals	Accomplishments
Issue a Notification letter or resolve a matter within 6 days, 80% of the time.	10 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.	48 days, 80% of the time.
Issue a Report or resolve a matter regarding a breach of privacy within 65 days, 80% of the time.	62 days, 80% of the time.
Complete or close Consultation files within 10 days, 80% of the time.	9 days, 80% of the time.
Develop a database to track the provision of summary advice by the office.	A case file management system has been designed and will be implemented in the Spring of 2018.
Explore the feasibility of a case records management system.	A case file management system has been designed and will be implemented in the Spring of 2018.
Develop with eHealth Saskatchewan audit and monitoring guidelines for trustees.	A guideline was developed jointly with eHealth Saskatchewan (see *Audit and Monitoring Guidelines for Trustees*).

The Plan 2018-2019

Education and Awareness

- Maintain the dictionary of access and privacy terms.
- Develop and post an "Access Impact Assessment" resource to assist public bodies to undertake open government initiatives.
- Develop and post guidelines on protecting personal information outside of the office.
- Develop and conduct a webinar question and answer period for Medical Clinics.
- Redesign and update the *IPC Guide to Exemptions for FOIP and LA FOIP*.
- Audit government websites to determine which ones have adequate access and privacy notices, policies and procedures.
- Promote and participate in a project with the Ministry of Justice and the Public Service Commission (PSC) to take the four PSC modules and convert them to LA FOIP terminology and make them available to local authorities.
- Develop and post a guide for public bodies in utilizing an extension of time to respond to the Applicant under section 7 of FOIP and LA FOIP.
- Develop and deliver a workshop/webinar on how to work with the IPC during a review.
- Finalize and post Rules of Procedure.
- Update the *IPC Guide to HIPA*.
- Update the resources for MLA's and Ministers.
- Develop and deliver a workshop/webinar for elected MLAs.

Navigating in a Digital World

- Develop and post guidelines for the use of mobile devices (BYOD, Texting) by health professionals.
- Develop and post a best practices guide for using social media.
- Develop and post a best practices guide for organizations on the use of memory sticks.
- Develop and post a report regarding the use of computer backup tapes.

Advocating for Improvement

- Propose and develop regulations for *The Data Matching Agreements Act*.
- Promote publicly funded bodies who are landlords to be under FOIP or LA FOIP.
- Promote a broader definition of trustee under HIPA or other legislation.

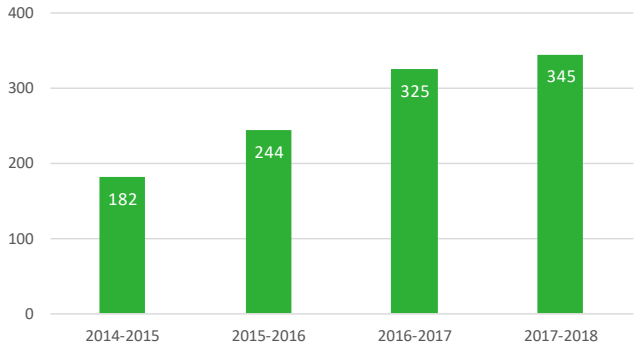
Effective While Efficient

- Issue a notification letter or resolve a matter within 20 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 a breach of privacy within 75 days, 80% of the time.
- Complete or close consultation files within 30 days, 80% of the time.
- Respond to an Application to Disregard within 20 days, 80% of the time.
- Implement a case file management system.
- Organize and deliver a National Information and Privacy Commissioners' Conference in September 2018.

Files and Reports

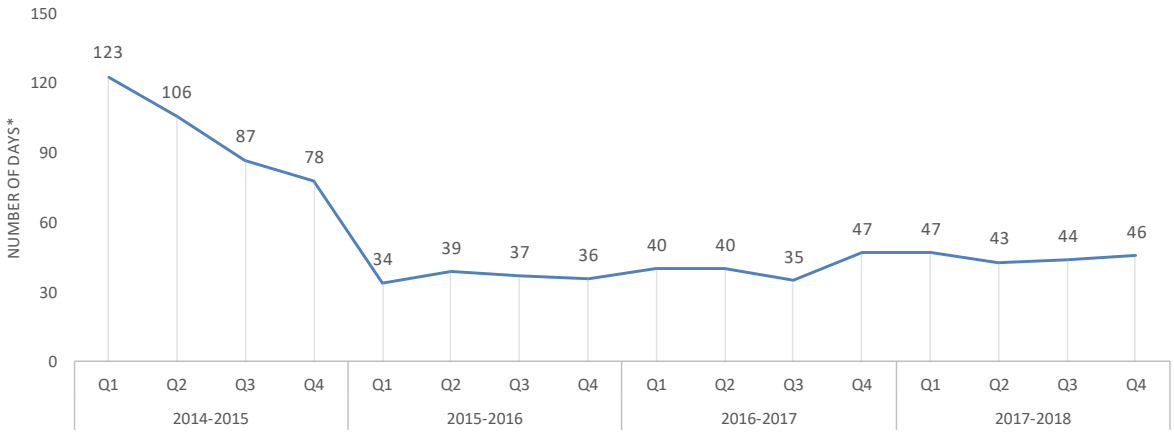
Increase in Files

The office is experiencing an increase in reviews, investigations and consultations, resulting in more files being opened as is reflected in the bar chart. This resulted in a 6% increase over the previous fiscal year.

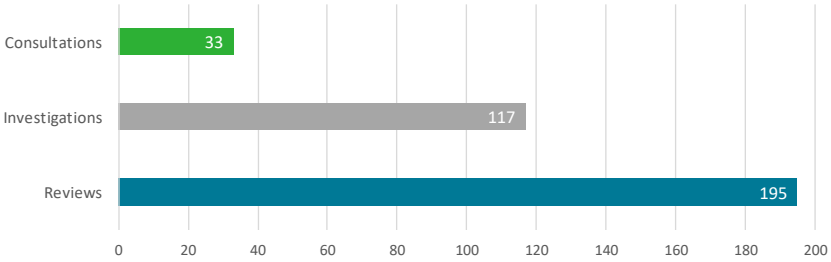


Response Time

The office has worked hard to improve its response time to citizens and public bodies. In 2017-2018, the response time increased mainly due to a 6% increase in files opened.



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

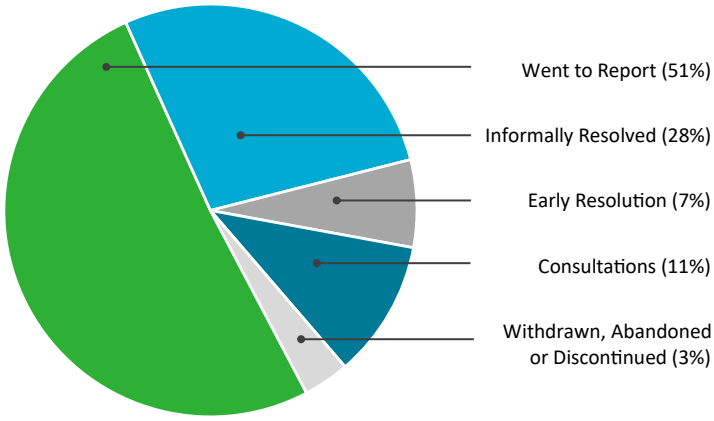


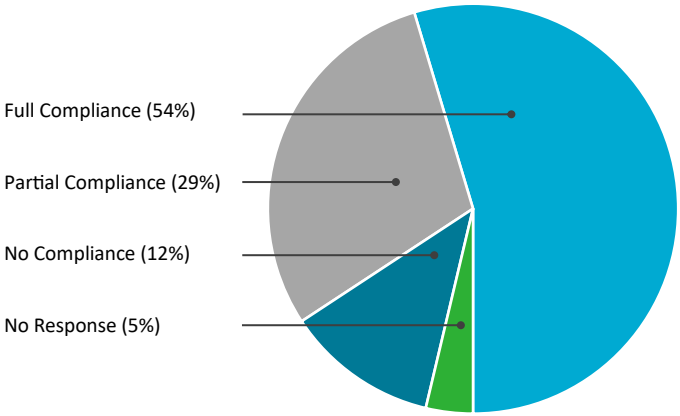
Types of Files Opened

The office opened 345 files in the 2017-2018 fiscal year. This is a chart summarizing the types of files opened.

Resolution of Files

The office closed 307 files in the 2017-2018 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 110 Reports in 2017-2018. A public body or trustee is required to respond to the recommendations within 30 days of receiving the Report. This 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 subsection 62(2) of FOIP, subsection 52(2) of LA FOIP and subsection 60(2) of HIPA.

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 or partially complied with*
Executive Council	Review Report 051-2017	[38]
Executive Council	Review Report 204-2016	[40]
Ministry of Health	Review Report 326 to 332-2017	[17]
Ministry of Highways and Infrastructure	Investigation Report 224-2016	[62]
Ministry of Highways and Infrastructure	Review Report 263 to 268-2016	[91], [93]
Ministry of Highways and Infrastructure	Review Report 289-2016	[35]
Ministry of Highways and Infrastructure	Review Report 032-2017	[37]
Ministry of Highways and Infrastructure	Review Report 055-2017	[40]
Public Complaints Commission	Review Report 276-2017	[44]
Saskatchewan Government Insurance	Review Report 104-2017	[80], [81]
Saskatchewan Government Insurance	Review Report 213 and 286-2017	[39]
Saskatchewan Legal Aid Commission	Investigation Report 226-2017	[46]
SaskPower	Review Report 025-2017	[34]
SaskPower	Review Report 139-2017	[111], [112]
Saskatchewan Water Security Agency	Review Report 236-2017	[62]
Saskatchewan Workers' Compensation Board	Investigation Report 266-2017	[46]
Local Authority	**Report #**	**Recommendation(s) not or partially complied with***
City of Regina	Review Report 215-2017	[29]
City of Saskatoon	Review Report 036-2017	[24]
City of Saskatoon	Review Report 102-2017	[74]
City of Saskatoon	Review Report 210-2017	[49]
Good Spirit School Division	Investigation Report 230, 237, 238 and 240-2017	[47], [50]
Regina Roman Catholic Separate School Division	Review Report 211-2017	[129]
R.M. of Manitou Lake	Review Report 156 and 264-2017	[108], [112]
R.M. of Rosthern	Review Report 031-2017 Part I	[49], [50]
R.M. of Rosthern	Investigation Report 086-2017	[43], [44]
Town of Ituna	Investigation Report 114-2017	[38]

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

Partial Compliance

Trustee	Report #	Recommendation(s) not or partially complied with*
Kelsey Trail Regional Health Authority	Investigation Report 124 and 135-2017	[56]
Regina Qu'Appelle Regional Health Authority	Investigation Report 096-2017	[37], [38]
Saskatchewan College of Paramedics	Investigation Report 021, 067, 068-2017	[120], [124], [125]
Saskatoon Regional Health Authority	Investigation Report 223-2017	[43]
Sherbrooke Community Centre	Investigation Report 077-2017	[46]
Sun Country Regional Health Authority	Investigation Report 103-2017	[29]

***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*
Executive Council	Review Report 205-2016	[77], [78]
Ministry of Highways and Infrastructure	Review Report 026-2017	[25], [26]
Ministry of Justice	Investigation Report 249-2017	[41]
Public Complaints Commission	Review Report 132-2017	[19]
Public Complaints Commission	Review Report 242-2017	[35]
Public Complaints Commission	Review Report 252-2017	[15]
Saskatchewan Government Insurance	Review Report 063-2017	[21], [22]
Saskatchewan Legal Aid Commission	Investigation Report 299-2017	[32], [33], [34]
Local Authority	**Report #**	**Recommendation(s) not complied with***
City of Saskatoon	Review Report 037-2017	[25]
R.M. of Blaine Lake	Review Report 075 and 076-2017	[44] to [50]
R.M. of Blaine Lake	Review Report 143-2017	[22], [23]
Trustee	**Report #**	**Recommendation(s) not complied with***
Prince Albert Parkland Regional Health Authority	Investigation Report 136-2017	[44], [45]
Saskatoon Regional Health Authority	Review Report 125-2017	[38]

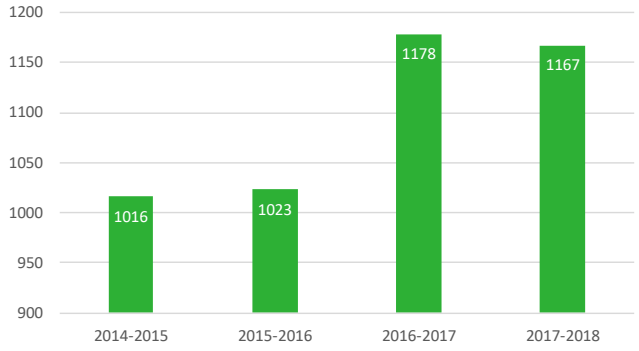
***Refers to paragraph # in the Report. Click on the link to go directly to the Report.**

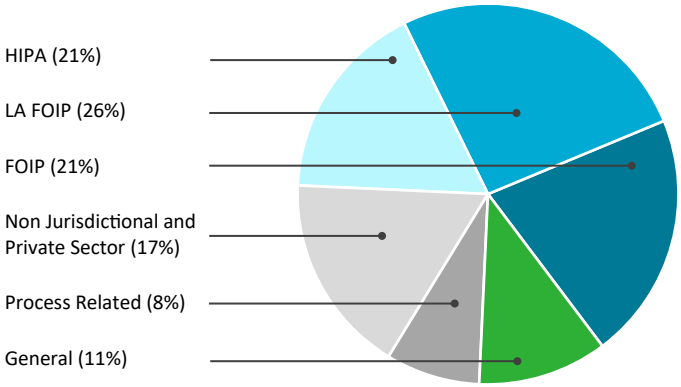
No Response Received		
Government Institution	**Report #**	**Recommendation(s) not complied with***
Ministry of Justice	Review Report 311-2016	[21]
Local Authority	**Report #**	**Recommendation(s) not complied with***
R.M. of McKillop	Review Report 082-2017	[49], [50]
Trustee	**Report #**	**Recommendation(s) not complied with***
Keewatin Yatthe Regional Health Authority	Investigation Report 230-2016	[55] to [63]
North-East EMS	Investigation Report 021, 067, 068-2017	[118], [119], [124]
Regina Physician Group	Investigation Report 305-2017	[44], [45], [46]

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

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 2017-2018, the office provided summary advice on 1167 occasions.





From the chart to the left, it is clear that the office gives advice related to the three main statutes where the office has jurisdiction; 64% of summary advice was given related to these pieces of legislation.

Reducing the Risks

In life, we all try to reduce the risk. We try to exercise, eat healthy, stop smoking, and not text while driving. All for the purpose of living longer and staying healthy. Reducing the risk applies in the access and privacy world, particularly since we have become so digital. This year I wanted to touch on a few topics where I ask government institutions, local authorities, trustees and third parties to think about their digital world and how they can reduce the risks of breaches of privacy.

We have all heard of significant breaches. They can be caused from within, outside or a combination of both. Finding an action that would guarantee total protection of privacy is near impossible. Complying with the legislation does not require perfection. Rather, what is required is for the public body to take reasonable measures to try to prevent privacy breaches. It is wise to take steps to reduce the risks of breaches of privacy. If an organization can do it in one step, great. But more likely it will take a series of steps over a period of time and doing some things on an annual basis. Often these steps include taking some preventive measures to identify threats and vulnerabilities, choosing specific controls and testing them to ensure they work to protect the personal information, developing and implementing broad policies to manage personal information throughout its life cycle and implementing ways to monitor whether any controls and policies need to be adjusted over time. In addition, new challenges and security risks will arise not known to us now that will heighten the risk and reinforce the need for action.

Below are just some examples where organizations can decrease the risk. In particular, starting with preventive measures, coupled with implementing specific controls including comprehensive policies and procedures, privacy breaches should be less likely to occur.

Prevention

Identify the information

Knowing what personal information exists, where it is stored and how it is being used is a key first step in identifying possible threats and areas of vulnerability. Understanding the context and sensitivity of the information can assist with identifying the specific controls that will be needed to protect the information.

Privacy Impact Assessment (PIA)

When an organization develops a new program, direction, service or computer system, the organization should consider conducting a privacy impact assessment. Obviously, the focus here is on privacy and the risks of collecting, using, protecting or disclosing information. In such a process, an organization looks at the risks or threats of the new program or system. Such an early analysis of the risks can in fact reduce the risk of privacy breaches in the future.

New Employees

When a new employee is hired by your organization, does that employee get privacy training? Is that employee required to read and acknowledge that they have read your privacy policies? Is that employee required to take an oath of confidentiality or sign a confidentiality statement? We recommend all of the above.

Annual Mandatory Training

My office advocates mandatory annual training for all staff. This is mainly to learn the rules of access by citizens to information, but also to lay out the rules on privacy. Public bodies have an obligation to protect personal information and that means having a computer system that has good security controls and staff knowing what they can do and cannot do. Also in the digital world, things change in a year, and staff need to hear the latest best practices to protect your organization.

Confidentiality Statements

Do you have your staff regularly re-visit their promises to the organization regarding confidentiality? Regular reminders regarding confidentiality are essential. Staff need to know about the "need-to-know" principle, which says, only provide personal information or personal health information to those who **need-to-know**. When staff provide others in their organization with personal information or personal health information they should provide the least amount of information necessary for the purpose. This is known as the "data minimization principle". Does personal information or personal health information get exchanged at the water cooler, coffee break, in the hallway or at the bar? In other words, when information is exchanged, is it done at a place and time that is appropriate?

Data Minimization

Similarly, employees should only collect, transfer and view information that they need, to do their job or solve the problem they have. Less information shared reduces the risk of that information being inappropriately disclosed. Computer systems, policies and training can be adjusted to reduce the risks of too much data being shared.

Specific Controls

Passwords

There are many articles out there about passwords. Some say change it periodically but others say develop a longer one that means something special to you and keep it. Do not share it and let someone else access the program or system with your password. All the advice certainly insists that we use strong passwords and keep those passwords to ourselves.

Letting Others Use Your Computer

We have heard things like it is easier to unlock the computer in the morning and let everyone use that computer. Organizations need to find ways that make this not necessary. In fact, they should go further and prohibit it by policy. Sharing passwords or computers can easily lead to an employee accessing information that they have no right to access.

Automatic Lockout

We all walk away from our computer screens. We should log out before we do so, but we frequently forget. It is important that if we are away for a number of minutes, the computer should just lock anyway. The IT unit should impose this requirement on all of us.

Two Smart Phones

If you have multiple email accounts and one smart phone, and you forward all emails to your smart phone, you are placing work emails at risk. Are the work emails saved in the right place? If your partner or children have access to your smart phone, they will have access to work information, which is very

inappropriate. The answer to reducing the risk is two smart phones, one as your work phone synchronized with your work server and one for personal use. Your work emails, etc. are then totally separated from your personal emails. You can let your children play with your personal smart phone without worry that they may access work information.

Encryption of Emails and Documents

Have you checked lately if your documents and emails are encrypted? If not, why not? It is a simple step to reduce the risk of those documents or emails being read. When you send a document to someone else and that document contains sensitive information, do you make the document password protected? Again, a simple step to reduce the risk of inappropriate disclosure.

Patches

Software manufacturers discover weaknesses in their programs and issue notices and patches. These patches can prevent security breaches. Delay in installing the patches is risky. Reduce the risk and install patches right away. A Panama law firm failed to keep software up to date and paid a significant price in terms of a massive privacy breach.

The Cloud

At one time, I was nervous about using the Cloud. Particularly when data would be saved in another country. Cloud providers have installed server farms in Canada, so that is less of a concern. These server farms are being operated by very large corporations and they are investing significant sums of money. It is coming to the point where using the Cloud may be cheaper and more secure. One provider has 1500 different security controls. It is time to look at your organization and determine which would be more secure, and assess which would be better suited for your purposes.

Daily Backups

Your computer system and the data it holds is valuable to the organization and the data can contain personal information and personal health information. Do you know if your IT staff or your information management service provider (IMSP) is doing daily backups? If your system has a malware attack or is a victim of ransomware, the main way to restart is to rely on your latest backup. If you do not have one, you are in trouble. So to reduce the risk, ensure that daily backups are taken and a total restoration can be achieved from the backup.

Backups on Tape

Traditionally computer systems backed up their data on magnetic tapes. The theory was that you would have a cycle and, after a month or two, the tape would be re-used and the old data was gone. In some instances, organizations began keeping the tapes much longer. The magnetic tapes can deteriorate and, over time, the data was vulnerable, not readable or recoverable at a considerable expense. Switching backup systems to store the data on disk or in the Cloud may allow greater certainty that the data will still be accessible. Organizations can reduce the risk by first deciding that backup systems are not part of the official records of an organization and should be treated as fulfilling a need of restoring a computer system. Of course, official records need to be stored and destroyed in accordance with the law and the archiving policies of the organization.

Policies

Business and Personal Emails

Risks can be reduced by separating your personal work from your business or organizational work. It takes a bit of thinking but it can be done. Have an email account for work, another for business and another for personal. If you

receive a work email on your personal account, forward it to your work account and then reply. Then everything will be stored where it should be. If it is work related, it is then stored and destroyed according to the retention policies of your organization.

Fax or Email

Are you still faxing documents which contain personal information or personal health information? Do some of those faxes go astray? That is a privacy breach. You need rigorous rules about fax numbers and you need to think about scanning the document and emailing it. Encrypted email reduces the risk of information getting into the wrong hands. But if an email does, encryption prevents others from reading it.

USB and Flash Drives

Do you allow staff to use USB drives, flash drives or thumb drives? Personal information may be walking out your front door every night. What if the drive is lost or stolen? Is it encrypted or password protected? Do you have a policy on who can do this and who cannot? Do you let staff use any old thumb drives or just thumb drives issued by the organization with encryption functionality?

Paper Files

Can staff take paper files home with them? Do you have a policy on who can and who cannot? Are there things you can do to reduce the risk of loss of paper files or theft from vehicles or homes? In fact, taking material on an encrypted USB drive is safer than taking it home in paper form.

Laptops

People have to travel to do their work. They may take a laptop with them. Do you have policies on who can and who cannot take a laptop? Is the laptop password protected? Is the data encrypted? Alternately, instead of having data on the laptop, can staff VPN into their office when they need the data. VPN reduces the risk of loss or theft of the laptop and personal information going missing. If you leave your laptop unattended, is it secured in a locked desk drawer or room? Can you prevent it from walking away?

Need-to-Know

The privacy world has a principle, need-to-know. It means an employee in an organization only has access to, and should only access information, that they need-to-know to do their job. Computer systems can limit what a staff person can access and training can emphasize that one should only access information when they need-to-know. Policies can indicate who has a need to know. These steps can reduce the risk of an employee inappropriately accessing information.

Personal Devices at Work

Most personal devices these days can take pictures of documents, of events, of clients, of patients and of other employees. Do you have a policy in place that sets out the rules on personal devices including when pictures can be taken and when they cannot? Having one is just another way to reduce the risk of a privacy breach. It is relatively easy for employees to forward emails from their work accounts to their personal device. Do you have policies restricting such a practice? It is also easy for one employee to text another employee on a personal device. Do you have policies regarding work related texts being sent to and from personal devices?

Organization Owned Devices

Does your organization issue smart phones or tablets to staff? These devices can also take pictures and videos. Do you have policies on how these devices will be used? If your organization sees customers or patients, do you have policies relating to pictures and videos of your customers or patients?

Again, texting on a smart phone is a common way of communicating. Do you have policies as to whether staff can text one another on organization devices regarding work issues? If such texts are allowed, do you have policies on how those texts are captured as part of the file or the record?

People in the workplace will text on their or the organization's mobile device. Some of those texts will be regarding business matters. Some of those texts will contain personal information or personal health information. Does your organization view those texts as part of the official record? How do you store those texts and how do you retrieve them. Does your organization have a policy either prohibiting text for work related matters or setting out the rules for storage and retrieval? See our guideline *Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools*.

Destruction of Official Records

If a system is breached, the intruder or snooper gets access to all the personal information and personal health information that is there. If records should have been destroyed, but have not, the intruder is getting information that should not have been there. Part of protecting my personal information is to destroy it when the rules of an organization dictates it should be destroyed. You can reduce the magnitude of the risk of a privacy breach by implementing proper retention and destruction practices in accordance with organization rules, policies and any applicable legislation.

Monitoring and Taking Action

Auditing Program

Organizations today rely heavily on our electronic systems. We need to give our employees access to our systems. New systems can be designed to precisely control who gets access to what. Old legacy systems have less flexibility in controlling access. Whether old or new, a way to reduce risk is to develop an audit plan, which includes logging who has accessed where and when, which consists of random checks and automated checks. All efforts in this regard will expose employee unauthorized access sooner and should act as a deterrent to those tempted to snoop.

The Love Triangle

My office has done a number of reports where a person, the ex-partner, snoops on the new spouse or partner. There is no need-to-know. It appears to be a great temptation that ex's cannot resist. Thus, this becomes a vulnerable point for our electronic systems. Through policy, training, confidentiality statements, monitoring and discipline is how employees realize the cost of submitting to temptation.

When the Privacy Breach Occurs

When a privacy breach occurs, particularly an external breach, you need to act quickly. Not tomorrow, but today. There is no time to develop a plan; the plan has to be there. Who do you call first, second, and third? What to do first, second and third. This is all about reducing the impact of the breach. To reduce the risk ensures your organization has a plan that can be implemented immediately.

Report to a Professional Association or Regulatory Body?

At times the person who committed the privacy breach belongs to a professional health organization. Most professional associations have a code of ethics and high standards on confidentiality. Your organization can consider reporting the person committing the breach to the professional association that the person is a member of. The professional association can then consider whether it wishes to take any action. This is just another way of an organization saying privacy breaches are unacceptable and there will be consequences.

The Disciplinary Process

If an organization has policies, training and confidentiality statements, and an employee still snoops, then the discipline process is the next risk reduction step. Over time, the consequences of snooping need to result in higher suspensions. Excessive snooping needs to result in termination. All of this is necessary to send a message to all that snooping is not tolerated.

Requesting a Prosecution

From time to time in a report by my office, it is recommended that the matter be referred to the public prosecutions office. There are times when the breach is so egregious that an organization should consider the triggering of the criminal process. Being charged with an offense and being convicted is certainly a deterrent. When it occurs, it should cause all of us to think about our conduct in the workplace. I would ask organizations in egregious situations to consider reporting the matter to public prosecutions in the Ministry of Justice.

Risk Reduction Strategy

Today, many organizations have a risk reduction strategy or process. It can be a longer term process to mitigate the risks faced by an organization. Does your organization include in its risk reduction strategy a privacy component where consideration is given to reducing the risks of a privacy breach?

Senior Level Meetings

Do you raise the issue of security and safeguards of information at senior level meetings? Do you discuss the issue in the context of reducing the risk of breaches internal or external? If not, reduce the risk of privacy breaches occurring by creating a culture of protecting personal information and personal health information.

Loss of Reputation

The Privacy Commissioner of Canada has said, "There is little more precious than our reputation." We have seen large organizations in Canada and the United States lose in the reputation area. They may have spent 20 plus years developing their brand and creating trust and, in one single breach, a major loss of reputation has happened. It is essential for organizations to protect their image and reduce the risk of reputation damage.

A Culture of Privacy

As we think about all the things that an organization can do to reduce the risk of privacy breaches, the best thing is for an organization to work on the culture of privacy. If an organization sends out many signals that privacy is important then the staff in that organization, over time, will accept that privacy is a value of that organization. Once all staff in an organization accept that privacy is important, the risk of a privacy breach will be reduced. This is the closest thing to a silver bullet when it comes to reducing risks of a privacy breach.

Conclusion

In our digital world, we will never have total security; our obligation is to take steps now that reduce the risk of personal information or personal health information ending up in the wrong hands.