Office of the
Saskatchewan Information
and Privacy Commissioner

GUIDE TO LA FOIP

The Local Authority Freedom of Information and Protection of Privacy Act

Chapter 6

Protection of Privacy

TABLE OF CONTENTS

Overview

The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP) provides a right of access to all records under the possession or control of local authorities, subject to limited and specific exemptions. Some of the records to which LA FOIP applies contain personal information, such as the employment history, family status or sexual orientation of an individual. Applicants often ask local authorities for access to records that contain the personal information of someone other than the applicant.

LA FOIP establishes several obligations on local authorities in terms of protecting personal information that the local authority collects, uses or discloses. This Chapter will assist with explaining those obligations and how to handle situations where an individual's privacy may have been breached.

What follows is non-binding guidance. Every matter should be considered on a case-by-case basis. This guidance is not intended to be an exhaustive authority on the interpretation of these provisions. Local authorities may wish to seek legal advice. Local authorities should keep section 51 of LA FOIP in mind. Section 51 places the burden of proof for establishing that access to a record may or must be refused on the local authority. For more on the burden of proof, see the *Guide to LA FOIP*, Chapter 2, "Administration of LA FOIP". **This is a guide**.

The tests, criteria and interpretations established in this Chapter reflect the precedents set by the current and/or former Information and Privacy Commissioners in Saskatchewan through the issuing of Review Reports. Court decisions from Saskatchewan affecting The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP) will be followed. Where this office has not previously considered a section of LA FOIP, the Commissioner looked to other jurisdictions for guidance. This includes other Information and Privacy Commissioners' Orders, Reports and/or other relevant resources. In addition, court decisions from across the country are relied upon where appropriate.

This Chapter will be updated regularly to reflect any changes in precedent. This office will update the footer to reflect the last update. Using the electronic version directly from our website will ensure you are always using the most current version.

The Right of Privacy

LA FOIP has two fundamental components: the right to access information and the protection of personal privacy. Part II of LA FOIP deals with access to records. Part IV of LA FOIP deals with protection of personal privacy.

Privacy is defined as the general right of the individual to be left alone, to be free from interference, from surveillance and from intrusions. It is the right of an individual to be able to control access to, as well as, the collection, use and disclosure of their personal information. Privacy captures both security and confidentiality of personal information.[1]

Privacy connotes concepts of intimacy, identity, dignity, and integrity of the individual.[2]

Protection of personal privacy means that individuals have a right to privacy of their personal information that is held by local authorities. To achieve this, LA FOIP establishes restrictions on the collection, use and/or disclosure of personal information. The provisions that address these restrictions are found at Part IV of LA FOIP.

LA FOIP promotes transparency, openness and accountability. Holding local authorities to account is important for democracy. Decision-makers must balance this important objective with the competing objective of the right to privacy. Privacy rights and the role of protection of personal information also play a role in a free and democratic society.[3] In *R. v. Dyment*, 1988 CanLII 10 (SCC), [1988] 2 SCR 417, Justice LaForest stated:

> 22. Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it (p. 13): "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of

[1] Office of the Saskatchewan Information and Privacy Commissioner (SK OIPC) *2012-2013 Annual Report* at Appendix 3, Definitions p. 100. See also SK OIPC Dictionary.
[2] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII), [2007] 1 FCR 203 at [52].
[3] *Hans v. STU*, 2016 NBKB 49 (CanLII) at [20].

information collected by them to those for which it was obtained; see, for example, the *Privacy Act*, S.C. 1980-81-82-83, c. 111.

23. One further general point must be made, and that is that if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. This is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated … Here again, Dickson J. made this clear in *Hunter v. Southam Inc*. After repeating that the purpose of s. 8 of the *Charter* was to protect individuals against unjustified state intrusion, he continued at p. 160:

> That purpose requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place. This, in my view, can only be accomplished by a system of prior authorization, not one of subsequent validation.[4]

Privacy is regarded as a fundamental right that is essential to safeguard the autonomy and dignity of an individual.[5]

Privacy is protected in LA FOIP by:

- Giving individuals a right of access to their own personal information and the opportunity to request corrections to it (s. 30 and s. 31).
- Requiring local authorities to collect personal information only where authorized by law (s. 24).
- Requiring local authorities to collect personal information directly from the individual, unless where authorized to collect it indirectly (s. 25).
- Requiring local authorities to inform individuals of the purpose for which the information is collected (when collected directly) (s. 25(2)).
- Requiring that local authorities use personal information that is accurate and complete when making a decision about an individual (s. 26).
- Requiring local authorities to establish policies and procedures to maintain administrative, technical and physical safeguards for personal information (s. 23.1).
- Limiting a local authority's use and disclosure of personal information to the purpose for which it was collected, a consistent purpose, another purpose with consent or a purpose set out in LA FOIP (s. 27).

---

[4] *R. v. Dyment*, 1988 CanLII 10 (SCC), [1988] 2 SCR 417 at [22] and [23].
[5] SK OIPC Investigation Report F-2005-001 at [22].

- Enabling individuals to make complaints to the Commissioner and empowering the Commissioner to investigate complaints regarding possible collection, use or disclosures in contravention of Part IV of LA FOIP (s. 32 and s. 38(1)(a.4)).
- Requiring local authorities to notify individuals of an unauthorized use or disclosure of the individual's personal information if there is a real risk of significant harm to the individual (s. 28.1).
- Providing fines and/or imprisonment to any person who knowingly collects, uses or discloses personal information in contravention of LA FOIP (s. 56).[6]

Privacy as a Charter Right

The Supreme Court of Canada has considered the concept of privacy in several different contexts and determined that the Canadian *Charter of Rights and Freedoms* guarantees all Canadians a right of privacy.[7]

The right of privacy is founded on sections 7 and 8 of the *Charter*. Those sections provide as follows:

7. *Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.*

8. *Everyone has the right to be secure against unreasonable search or seizure.*[8]

Section 8 of the *Charter* is intended to protect individuals from unjustified state intrusions upon their privacy. The scope of section 8 is limited by the reasonableness of the individual's expectation of privacy in a given set of circumstances.[9]

The Supreme Court of Canada has recognized several kinds of privacy namely, physical, or bodily privacy, territorial privacy, privacy of communications and information privacy. For purposes of LA FOIP, the focus is only on information privacy. The Supreme Court of Canada has quoted with approval the following statement:

---

[6] Adapted from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, pp. 2 to 3.
[7] SK OIPC Investigation Report F-2005-001 at [21].
[8] *The Constitution Act, 1982*, Schedule B to the *Canada Act 1982* (UK), 1982, c 11. Also quoted in SK OIPC Investigation Report F-2005-001 at [23].
[9] *Hunter et al. v. Southam Inc.*, 1984 CanLII 33 (SCC), [1984] 2 SCR 145 at p. 160.

This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.[10]

For the privacy rights to be engaged at Part IV of LA FOIP, the information must constitute personal information under subsection 23(1) of LA FOIP. To help determine this, see *Definition of Personal Information* later in this Chapter.

IPC Findings

In Review Report F-2005-001, the Commissioner investigated the practice of the Automobile Injury Appeal Commission (AIAC) of publishing on its website the full text of its decisions. Those decisions included a good deal of personal information of those persons applying for compensation. The Commissioner found that there was no legislative requirement that the AIAC publish decisions on its website and that such publication falls short of privacy 'best practices'. Part of the investigation involved the Commissioner considering whether "privacy" was a right under the Canadian *Charter of Rights and Freedoms*.

Privacy versus Confidentiality

The words "*confidentiality*" and "*privacy*" do not mean the same thing:

Confidentiality is the protection of personal information, once obtained, against improper or unauthorized use or disclosure. This is just one aspect of privacy and is not synonymous with "privacy". It is the duty to protect personal information.[11]

Privacy is a broad concept that involves the right of the individual to exercise a measure of control over their personal information. It involves the decision of the individual as to what personal information will be disclosed to a local authority and for what purposes. Privacy captures both the security and confidentiality of personal information.[12] Privacy is the general right of the individual to be left alone, to be free from interference, from

[10] *R.v. Dyment* 1988 CanLII 10 (SCC), [1988] 2 S.C.R. 417 at [22]. Also quoted in SK OIPC Investigation Report F-2005-001 at [25].
[11] SK OIPC *Glossary of Common Terms: The Health Information Protection Act (HIPA)*. See also SK OIPC *2009-2010 Annual Report* at *Appendix 1 – Definitions*, p. 53.
[12] SK OIPC Investigation Report H-2013-001 at [193]. Originated from SK OIPC *Glossary of Common Terms: The Health Information Protection Act (HIPA)*.

surveillance and from intrusions.[13] It is about the individual being able to control access to, as well as collection, use and disclosure of, their personal information.[14]

Privacy may be defined as an individual's right to determine for themselves, when, how and to what extent they will release personal information about themselves. Privacy thus connotes concepts of intimacy, identity, dignity, and integrity of the individual.[15]

The Threat of Identity Theft

Identity theft refers to the collection or acquisition of someone else's personal information to conduct criminal activities.[16]

Identity fraud is the actual use of another person's information in connection with fraud. This includes impersonation and the misuse of debit or credit card information.[17]

Identity theft is one of the most serious crimes in Canada and one that has significantly increased in frequency and sophistication. Identity thieves will steal wallets, redirect mail, rummage through garbage, set up telemarketing schemes, break into computers to take money out of bank accounts, go on shopping sprees, apply for loans, credit cards and social benefits, rent apartments and even commit more serious crimes – all in the victim's name.[18]

---

[13] *R. v. Edwards* (1996), 103 C.C.C. (3d) 136 (S.C.C.) at paras. 49-50.
[14] *Privacy and Confidentiality of Health Information at CIHI: Principles and Policies for the Protection of Personal Health Information and Policies for Institution-Identifiable Information*, 3rd Edition, Ottawa: Canadian Institute for Health Information, April 2002, a p. 52. Referenced in SK OIPC Investigation Report H-2005-002 at p. 23.
[15] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII), [2007] 1 FCR 203 at summary on p. 2.
[16] Office of the Ontario Information and Privacy Commissioner (ON IPC) resource, *Ensuring your privacy is protected.* Available at https://www.ipc.on.ca/privacy-individuals/ensuring-your-privacy-is-protected/. Accessed on October 18, 2022.
[17] ON IPC resource, *Ensuring your privacy is protected.* Available at https://www.ipc.on.ca/privacy-individuals/ensuring-your-privacy-is-protected/. Accessed on October 18, 2022.
[18] Originated from former Saskatchewan Justice Minister, Frank Quennell's news release, *"Saskatchewan Supports Identity Theft Initiatives"*, March 12, 2004. Cited in SK OIPC Investigation Report H-2007-001 at [41].

In addition to names, addresses and telephone numbers, identity thieves look for social insurance numbers, driver's licence numbers, credit card and banking information, bankcards, calling cards, birth certificates and passports.[19] This personal information enable's an identity thief to commit various forms of fraud using the victim's identity, such as:

- Access bank accounts
- Apply for loans, credit cards and other goods and services
- Obtain new identity documents, such as passports
- Receive local authority benefits
- Hide criminal activities[20]

Once they steal the information they need, identity thieves can manipulate it and invade their victim's personal and financial lives. Victims of identity theft may incur damaged credit cards, unauthorized charges on credit cards and unauthorized withdrawals from bank accounts. In many cases, victims must change their address, telephone number and even their social insurance numbers.[21] It can take months or years to correct, and the consequences can be serious:

- Poor credit ratings
- Ruined reputations
- Lost jobs and other opportunities
- Services denied
- Loss of freedom to travel[22]

From the perspective of identity theft, one of the most important kinds of personal information is that which is contained in "cradle to grave" type information. Birth and death certificates are frequently used as foundation documents to establish identity. According to

[19] Originated from former Saskatchewan Justice Minister, Frank Quennell's news release, *"Saskatchewan Supports Identity Theft Initiatives"*, March 12, 2004. Cited in SK OIPC Investigation Report H-2007-001 at [41].
[20] ON IPC resource, *Ensuring your privacy is protected.* Available at https://www.ipc.on.ca/privacy-individuals/ensuring-your-privacy-is-protected/. Accessed on October 18, 2022.
[21] Originated from former Saskatchewan Justice Minister, Frank Quennell's news release, *"Saskatchewan Supports Identity Theft Initiatives"*, March 12, 2004. Cited in SK OIPC Investigation Report H-2007-001 at [41].
[22] ON IPC resource, *Ensuring your privacy is protected.* Available at https://www.ipc.on.ca/privacy-individuals/ensuring-your-privacy-is-protected/. Accessed on October 18, 2022.

the Royal Canadian Mounted Police (RCMP), two of the three "key pieces of information" sought by the suspects to build a profile are name and date of birth.[23]

The RCMP has noted that the following are pieces of information identity thieves seek:

- Full name
- Date of birth
- Social Insurance Number
- Full address
- Mother's maiden name
- Username and password for online services
- Driver's licence number
- Personal identification numbers (PIN)
- Credit card information (numbers, expiry dates and the last three digits printed on the signature panel)
- Bank account numbers
- Signature
- Passport number[24]

Identity thieves use a variety of methods to obtain personal information:

Low-tech methods include:

- Searching through the garbage.
- Stealing or re-directing postal mail.
- Pretending to be someone else and requesting it, for example, telemarketing schemes.
- Opportunistic theft: accessing personal information sent to the wrong fax number, email address or voice mailbox.

High-tech methods include:

- Searching the internet; "friending" you on social media.

---

[23] Originated from former Saskatchewan Justice Minister, Frank Quennell's news release, *"Saskatchewan Supports Identity Theft Initiatives"*, March 12, 2004. Cited in SK OIPC Investigation Report H-2007-001 at [41].

[24] SK OIPC Investigation Report H-2013-002 at [18]. Originated from the Royal Canadian Mounted Police (RCMP) *Identity Theft and Identity Fraud*.

- Hacking ATMs and point-of-sale devices to steal your payment card information.
- Installing malware on your personal computing devices.
- Tricking you into visiting fraudulent websites via phishing messages.
- Intercepting and eavesdropping on your Wi-Fi communications.[25]

Local authorities should take all reasonable measures to protect personal information to reduce the risk of identity theft. This Chapter will set out several ways that local authorities can achieve this by having administrative, technical, and physical safeguards in place that protect personal information in the local authority's possession or control.[26] See *Section 23.1* later in this Chapter.

IPC Findings

In Investigation Report 009-2020, 053-2020, 224-2020, the Commissioner investigated a ransomware attack on eHealth Saskatchewan (eHealth), the Saskatchewan Health Authority (SHA) and the Ministry of Health (Health). As a result of the ransomware attack in late December 2019 and early January 2020, approximately 40 gigabytes of encrypted data were stolen from eHealth by malicious actors. Personal information and personal health information of individuals was involved. The Commissioner made several recommendations to assist eHealth, the SHA and Health against future attacks. This included that eHealth utilize key network security logs and scans to effectively monitor the eHealth IT network and detect malicious activity, undertake a comprehensive review of eHealth's security protocols to include in depth investigation when early signs of suspicious activity are detected, and eHealth require cyber security and privacy training be required for eHealth and its partners as part of new employee orientation and onboarding. In addition, the Commissioner recommended that eHealth, the SHA and Health review and amend IT acceptable use policies to include examples of current threats that employees should be aware of.

In Investigation Report 089-2021, the Commissioner investigated a ransomware attack on Saskatoon Obstetric & Gynecologic Consultants (SOGC). The attack affected 20,000 patients. Due to a lack of retention of system logs, SOGC was unable to fully investigate the breach and recommended SOGC develop and implement a policy and procedure or ensure the agreements with its IT service providers contain language regarding the retention of firewall

[25] ON IPC resource, *Ensuring your privacy is protected.* Available at https://www.ipc.on.ca/privacy-individuals/ensuring-your-privacy-is-protected/. Accessed on October 18, 2022.
[26] Section 24.1 of FOIP requires local authorities to establish policies and procedures to maintain administrative, technical, and physical safeguards that protect personal information in its possession or control. See section 24.1 later in this Chapter for more detail.

and network security logs, and that regular reviews of those logs are conducted to enable monitoring of SOGC's system. Several other recommendations were also made including ensuring it has a written agreement with its new IT service provider clearly outlining the services the IT service provider will provide.

10 Fair Information Principles

In 1980, the Organization for Economic Co-operation and Development (OECD) developed *Guidelines for the Protection of Privacy and Trans-border flows of Personal Data* (*OECD Guidelines*). The *OECD Guidelines* represented an international effort to balance effective privacy protection with the free flow of personal data between different countries.[27] The *OECD Guidelines* included eight principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. In 1984, Canada committed itself to privacy protection by signing on to these internationally recognized guidelines.

In 1995, the European Union (EU) issued a directive on data protection called the *European Union Data Protection Directive* (also known as *EC.95.46*). The *EC.95.46* was adopted by the EU to protect the personal data collected for or about citizens of the EU.[28] The Directive was based on the 1980 *OECD Guidelines*. The Directive effectively prohibited the trade by EU member nations with any jurisdiction that did not have adequate privacy protection. This put pressure on the international community to have adequate privacy protections in place or risk trading opportunities with the EU.

These early guidelines (*OECD Guidelines* and *EC.95.46*) and Canada's commitment to them formed the basis for the development of the *Canadian Standards Association Model Code for the Protection of Personal Information* (*Model Code*) in 1995. The *Model Code* was intended to be a voluntary tool to assist private businesses and organizations with managing the personal information of Canadians. When it was issued, it contained 10 principles that were referred to

[27] Organization for Economic Co-Operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed June 2, 2020.
[28] EUR-Lex, Access to European Union Law, *Summaries of EU Legislation, Protection of personal data*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14012. Accessed June 2, 2020.

as '*Fair Information Principles*'. It was thought that by implementing nationally recognized fair-handling practices for personal information, organizations could demonstrate their commitment to the protection of personal information in a material way.[29]

The *Model Code* came out of a collaborative effort by representatives of government, consumers, and business groups. These groups met and discussed the development of a code as a way of enhancing the business environment. These groups recognized protecting customers' privacy rights and treating personal information with respect offered a competitive advantage.[30]

The *Model Code* was initially designed for use by Canadian private businesses. However, the federal government incorporated the *Model Code* into the *Personal Information Protection and Electronic Documents Act* (PIPEDA) as Schedule 1 in April 2000. Canada was the first country in the world to have private sector privacy legislation that was based on a collaboratively developed national standard.[31] As well, the *Model Code* influenced the underlying concepts for all provincial access and privacy legislation in Canada, including Saskatchewan's LA FOIP Act.

The *Model Code* addresses two broad issues:

1. the way organizations collect, use, disclose, and protect personal information; and

2. the right of individuals to have access to personal information about themselves, and, if necessary, to have the information corrected.[32]

---

[29] Canadian Standards Association (CSA), *Model Code for the Protection of Personal Information (Q830)*. Available at https://www.csagroup.org/store/search-results/?search=all~~Q830. Accessed June 2, 2020.
[30] Office of the Privacy Commissioner of Canada, *An Overview of the Personal Information Protection and Electronic Documents Act for Businesses and Organizations*.
[31] Office of the Privacy Commissioner of Canada, *An Overview of the Personal Information Protection and Electronic Documents Act for Businesses and Organizations*.
[32] Canadian Standards Association (CSA), *Model Code for the Protection of Personal Information (Q830)*. Available at https://www.csagroup.org/store/search-results/?search=all~~Q830 . Accessed June 2, 2020.

The following are the 10 *Fair Information Principles* that are outlined in the *Model Code,* the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and form the underlying concepts of Saskatchewan's LA FOIP:[33]

Accountability

The *Model Code* states:

> An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Accountability is the first of the 10 principles in the *Model Code*. It is viewed as perhaps the most fundamental of all the principles and the foundation for the other nine. Accountability means the organization is accountable to the individual for the management of their personal information.

Organizations should delegate an individual or a team to be responsible for access and privacy related matters. The organization should have properly trained staff who specialize in the field of access and privacy. This allows for a contact point for individuals who wish to address a concern or ask a question related to their personal information. Without this, individuals are left unsure of where to take their issues and concerns and organizations are less accountable to citizens for how they manage personal information.

See Chapter 2: *Administration of LA FOIP, Local Authorities – Roles & Responsibilities; The LA FOIP Coordinator or Privacy Officer* for more information.

Identifying Purposes

The *Model Code* states:

> The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

---

[33] Canadian Standards Association (CSA), *Model Code for the Protection of Personal Information (Q830)*. Available at https://www.csagroup.org/store/search-results/?search=all~~Q830. Accessed June 2, 2020.

Individuals should be able to maintain a level of control over their own personal information. However, this is not possible if organizations are not clear and transparent about the reasons for collecting the personal information.

Consent

The *Model Code* states:

> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

One of the most prominent and distinctive features of the *Model Code* is that it is consent-driven. In other words, subject to limited exceptions, consent of the individual is required to collect, use or disclose personal information about that individual.

For more on consent, see *Consent Requirements*, later in this Chapter.

Limiting Collection

The *Model Code* states:

> The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting collection can only be accomplished if the purpose is clearly identified as stated in *Fair Information Principle* #2. Organizations should not collect more than what is necessary for the identified purpose. With advancements in technology, personal information is becoming more valuable, and organizations realize that personal information is a form of data currency.

For more on this topic, see *Over-collection* and *Data Minimization* later in this Chapter.

Limiting Use, Disclosure and Retention

The *Model Code* states:

> Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

In Investigation Report LA-2010-001, the Commissioner stated:

> [47] The practice of disclosing the least amount of information when required is called the 'data minimization principle'. This is one of the 10 Fair Information Principles that have been codified in the Canadian Standards Association *Model Code for the Protection of Personal Information* (Q830) …

For more on the data-minimization principle, see *Data Minimization* later in this Chapter.

Accuracy

The *Model Code* states:

> Personal information shall be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used.

Individuals have a right to have their personal information accurately reflected if collected, used and disclosed by an organization. Incorrect information can have tremendous consequences for individuals. Many jurisdictions have access and privacy legislation that provide individuals the right to have their personal information or personal health information corrected by organizations. Organizations should take measures to ensure that the personal information they are collecting, using and disclosing is accurate, complete and up to date. As well, they should provide for the ability of individuals to correct the information if it is not.

For more on accuracy and correction, see *Section 26: Standard of Accuracy* and *Section 31: right of correction* later in this Chapter.

Safeguards

The *Model Code* states:

> Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

If an organization is going to collect an individual's personal information, it has a responsibility to keep the information safe from improper use and disclosure. This includes physical, technical and administrative safeguards. Without these, privacy breaches can more easily occur. For example, physical safeguards would include properly locking file cabinets or offices that contain the personal information of individuals.

For more on safeguards, see *Section 23.1: Duty to Protect Personal Information* later in this Chapter.

Openness

The *Model Code* states:

> An organization shall make readily available to individuals, specific information about its policies and practices relating to the management of personal information.

Individuals need to be confident that their personal information is being collected, used, and disclosed properly, stored safely and is correct and accurate. Unless organizations are open about these things, individuals have no way of knowing what happens to their personal information once provided to an organization.

Individual Access

The *Model Code* states:

> Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

When an individual shares their personal information with an organization, they should not cease to have any control over it. They should be able to request access to it. In fact, access to one's own personal information is legislated in each jurisdiction in Canada.

Challenging Compliance

The *Model Code* states:

> An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Like *Fair Information Principle* #1, the ability to challenge compliance with these principles is important to accountability on the part of the organization. Each organization should have a designated individual or team that specializes in access and privacy principles and legislation. Individuals should have the ability to register complaints or concerns with organizations and they should be handled appropriately.

See Chapter 2: *Administration of LA FOIP, Local Authorities – Roles & Responsibilities; The LA FOIP Coordinator or Privacy Officer* for more information on the role of a Privacy Officer.

For more guidance on the *Fair Information Principles*, see the Office of the Privacy Commissioner of Canada's resource, *PIPEDA fair information principles*. Each of the principles is broken down further with tips and steps that can be taken to enhance the principle.

Need-to-Know Principle

Two principles flow from the 10 Fair Information Principles above:

1. The need-to-know principle (limiting collection, use & disclosure); and

2. The data minimization principle (identifying purpose, limiting collection, use & disclosure).

These two principles are implicit in Part IV of LA FOIP.

Need-to-know is the rule that personal information should only be available to those employees in an organization that have a legitimate need to know that information for the purpose of delivering their mandated services.[34]

The exercise of collecting, using, and disclosing personal information is always subject to the need-to-know principle.[35]

For a local authority to be able to rely on any provision in LA FOIP for its collection, use and/or disclosure of personal information, it must also abide by the need-to-know and data

[34] SK OIPC Investigation Report F-2009-001 at [92].
[35] Adapted from SK OIPC Investigation Report F-2009-001 at [47].

minimization principles. Authority to collect, use and disclose only exists when these principles are abided by. These two important principles underlie Part IV of LA FOIP.[36]

Identifying the 'need-to-know' requires careful consideration of what data elements are required and separating out those that are not required for the purpose identified. As well, organizations should only allow those that have a 'need to know' access to the personal information.

IPC Findings

In Investigation Report 074-2018, 075-2018, the Commissioner found that the disclosure of a complainant's personal information by a local authority was not appropriate because more personal information than was necessary for the purpose was disclosed. Even though the local authority had a provision to rely on and the discretion to disclose certain details, it did not adhere to the need-to-know and data minimization principles. Therefore, it did not have authority for the disclosures.

Data Minimization Principle

In Investigation Report LA-2010-001, the Commissioner stated:

> [47] The practice of disclosing the least amount of information when required is called the 'data minimization principle'. This is one of the 10 Fair Information Principles that have been codified in the Canadian Standards Association *Model Code for the Protection of Personal Information* (Q830) …

The data minimization principle is one of the 10 *Fair Information Principles*, which originated from the *Canadian Standards Association Model Code for the Protection of Personal Information* (*Model Code*). Specifically, principles #4 (Limiting Collection) and #5 (Limiting Use, Disclosure, and Retention). For more on this, see *10 Fair Information Principles* earlier in this Chapter.

Data minimization is the rule that an organization should always collect, use, and disclose the least amount of personal information necessary for the purpose.[37]

[36] SK OIPC Investigation Report 074-2018, 075-2018 at [38]. See also Investigation Report 278-2017 at [22].
[37] SK OIPC Investigation Report F-2009-001 at [92].

The exercise of collecting, using, and disclosing personal information is always subject to the data minimization principle.[38]

Disclosure is occasionally mandatory, but most often is a discretion for the local authority to exercise dependent on the particular circumstances. It is subject to the requirement to disclose the least amount of identifying information necessary for the purpose.[39]

For a local authority to be able to rely on any provision in LA FOIP for its collection, use and/or disclosure of personal information, it must also abide by the need-to-know and data minimization principles. Authority to collect, use and disclose only exists when these principles are abided by. These two important principles underlie Part IV of LA FOIP.[40]

IPC Findings

In Investigation Report LA-2010-001, the Commissioner found that a local authority disclosed more personal information than was necessary to the Canada Revenue Agency. As such, the Commissioner found that this constituted a breach of the complainant's privacy.

In Investigation Report 074-2018, 075-2018, the Commissioner found that the disclosure of a complainant's personal information by a local authority was not appropriate because more personal information than was necessary for the purpose was disclosed. Even though the local authority had a provision to rely on and the discretion to disclose certain details, it did not adhere to the need-to-know and data minimization principles. Therefore, it did not have authority for the disclosures.

De-identified information

Information is the new currency of our economy. Since the dawn of the digital era, information has become increasingly available, and at a scale previously unimaginable. With technological advances, this information is also becoming easier to collect, retain, use, disclose and leverage for a wide range of secondary uses.[41]

---

[38] Adapted from SK OIPC Investigation Report F-2009-001 at [47].
[39] SK OIPC Investigation Reports F-2007-001 at [82] and LA-2010-001 at [46]. See also Investigation Report 278-2017 at [22].
[40] SK OIPC Investigation Report 074-2018, 075-2018 at [38].
[41] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 1.

However, if organizations do not strongly protect the privacy of individuals in the information being sought out, there may be far-reaching implications for both the individuals and the organizations involved. For example, when individuals lose trust and confidence in the ability of an organization to protect their privacy, the reputation of that organization may be irreparably damaged in the process. This does not include the time and resources needed to contain, investigate, and remediate any resulting data breaches or privacy infractions, and the costs associated with any ensuing proceedings and liabilities such as class action lawsuits.[42]

One of the most effective ways to protect the privacy of individuals is through strong de-identification. Using proper de-identification techniques and re-identification risk management procedures, remains one of the strongest and most important tools in protecting privacy.[43]

De-identification is the general term for the process of removing personal information from a record or data set.[44]

De-identified information is information that cannot be used to identify an individual, either directly or indirectly. Information is de-identified if it does not identify an individual, and it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual.[45]

Personal information is de-identified through a process involving the removal or modification of both direct identifiers and indirect or quasi-identifiers.[46]

Direct identifiers are fields of information that may be used to directly identify an individual; they include name, home address, telephone number, health number and social insurance number.[47]

Indirect or quasi-identifiers are fields of information that may be used on their own or in combination with other indirect or quasi-identifiers, or other information, to indirectly identify an individual. They include information such as gender, marital status, race, ethnic origin, postal code or other location information, significant dates, or one's profession. Some indirect or quasi-identifiers may be more likely to lead to the re-identification of individuals in a data set due to their rare occurrence. Characteristics which are highly uncommon in the

---

[42] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 1.
[43] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 1.
[44] ON IPC resource, *De-identification Guidelines for Structured Data,* June 2016 at pp. 1 and 3.
[45] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 3.
[46] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 3.
[47] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 3.

population or in the data set, such as an unusual occupation or medical diagnosis, can increase the likelihood of the identity of an individual being revealed.[48]

Re-identification is any process that re-establishes the link between identifiable information and an individual.[49]

Masking is the process of removing a variable or replacing it with pseudonymous or encrypted information.[50]

De-identification protects the privacy of individuals because once de-identified, a data set is considered to no longer contain personal information. If a data set does not contain personal information, its use or disclosure cannot violate the privacy of individuals.[51] The privacy provisions of LA FOIP would not apply to de-identified information.

Removal of an individual's name alone does not necessarily qualify personal information as sufficiently de-identified. It is possible to re-identify an individual if information is publicly available. The ability to re-identify is increased when the information contains unique characteristics (e.g., unusual occupation, unusual death, or event) and the existence of external sources of records with matching data elements which can be used to link with the de-identified information (e.g., voter registration records, newspapers, obituaries, social media sites and other public registries). The risk of re-identification increases as the number of variables increases, as the accuracy or resolution of the data increases and the number of external sources increases.[52]

An **identifier** is information such as:

- A person's name
- Social Insurance Number
- Driver's license number
- Employee number
- Health card number
- Address
- Date of birth (usually used in combination with other identifiers such as name to distinguish between people with the same name but different birth dates)

[48] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 3.
[49] ON IPC resource, *De-identification Guidelines for Structured Data,* June 2016 at p. 2.
[50] ON IPC resource, *De-identification Guidelines for Structured Data,* June 2016 at p. 2.
[51] ON IPC resource, *De-identification Guidelines for Structured Data,* June 2016 at p. 1.
[52] SK OIPC Review Report F-2014-005 at [22] to [23].

- Any other discrete element of personal information that would enable a third party to deduce the identity of the person concerned.[53]

There are two types of identifiers:

Direct identifiers

Directly identifying variables can be used to uniquely identify an individual either by themselves or in combination with other readily available information. Examples can include name, telephone number or email address.

Indirect or quasi-identifiers

Indirectly identifying variables (quasi-identifiers) can be used to probabilistically identify an individual either by themselves or in combination with other available information. Examples can include sex, date of birth or postal code.[54]

Examples of quasi-identifiers can include sex, date of birth or age, geo-codes, first language, ethnic origin, aboriginal identity, total years of schooling, marital status, criminal history, total income, visible minority status, profession, health event dates, health-related codes, country of birth, birth weight, and birth plurality.[55]

Sufficient quasi-identifiers make it possible to identify an individual even in absence of a name, either on their own or in combination.[56]

---

[53] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[54] ON IPC resource, *De-identification Guidelines for Structured Data,* June 2016 at p. 4. See also Canadian Institute for Health Information (CIHI) resource, *Best Practice Guidelines for Managing the Disclosure of De-Identified Health Information* at pp. 12, 13 and 17.
[55] Canadian Institute for Health Information, *'Best Practice' Guidelines for Managing the Disclosure of De-Identified Health Information,* pp. 12, 13 and 17.
[56] Canadian Institute for Health Information (CIHI) resource, *Best Practice Guidelines for Managing the Disclosure of De-Identified Health Information* at pp. 12, 13 and 17.

The goal is to reduce the risk of re-identification of information once it has been de-identified. The following table shows decreasing probability of re-identification of information:[57]

State	Description
1. Identifiable data	The data have directly identifying variables or sufficient quasi-identifiers that can be used to identify the individual.
2. Potentially de-identified data	Manipulations have been performed on the identifying variables but attempts to disguise the quasi-identifiers may be insufficient. The data may not be fully de-identified, partially exposed, and may represent a re-identification risk.
3. De-identified data	An objective assessment of re-identification risk has been done and it is concluded that all directly identifying variables have been adequately manipulated and quasi-identifiers adequately disguised to ensure an acceptable level of re-identification risk.
4. Aggregate data	These are summary data such as tables or counts, where there are no identifying variables or quasi-identifiers.

For more on how to de-identify personal information, see the following resources:

Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy (June 2011, ON IPC)

De-identification Protocols: Essential for Protecting Privacy (June 25, 2014, ON IPC)

[57] Canadian Institute for Health Information (CIHI) resource, *Best Practice Guidelines for Managing the Disclosure of De-Identified Health Information* at pp. 12, 13 and 17.

De-identification Guidelines for Structured Data (June 2016, ON IPC)

IPC Findings

In Review Report LA-2013-003, the Commissioner found that the then Saskatoon Regional Health Authority (SRHA) severed the names, email addresses, mailing addresses, other contact information and the opinions submitted by private individuals. The Commissioner noted that once the name and contact information was severed from the record, the contents of the record would be sufficiently de-identified. Once information was sufficiently de-identified, it no longer was classified as personal information for purposes of LA FOIP and could be released.

In Review Report F-2014-005, the Commissioner considered the severing of names of teachers, the schools they worked, classes they taught and extra-curricular activities involved in and their work email addresses. This information was not considered personal information. However, the Ministry of Education had concerns about the linking of this information to other information that would reveal personal information of other individuals. The Commissioner considered whether it would be reasonable to expect that an individual may be identified if this information were disclosed. The Commissioner found that these pieces of information were unique identifiers that, if released, would make it more possible to identify a specific teacher involved in professional misconduct or incompetence and the name of the victim.

In Investigation Report 105-2014, the Commissioner found that direct and quasi-identifiers were being shared among participants of a Hub as part of Community Mobilization Prince Albert (CMPA). The Commissioner recommended that a comprehensive plan be developed and implemented to ensure deficiencies pertaining to agreements, policy, procedure, notice, training and documentation to ensure a consistent approach by all partner agencies. Further, the plan was to address, among other things, de-identification.

In Review Report 044-2017, the Commissioner recommended that Horizon School Division review records and de-identify information as much as possible. In some instances, the record could be de-identified by severing names of other students or parents. In other instances, de-identification may require removing portions or entire sentences. Further, the Commissioner recommended that Horizon School Division release the de-identified information regarding its investigation to the applicant.

Necessary, Effective & Proportional

When a local authority is considering a new initiative – such as a new service, program, activity, or legislation – that involves collecting, using, or disclosing personal information, a key concern is to achieve the appropriate balance between the benefits of the initiative and its impact on individual privacy.[58]

Put another way: if an initiative involves an intrusion into privacy, a local authority will want to consider whether the impact on privacy is 'reasonable and proportionate' in the circumstances.[59]

Following the enactment of the Canadian *Charter of Rights and Freedoms* in 1982, the Supreme Court of Canada formulated a methodological test to determine whether the violation of a *Charter* right is nonetheless justifiable in a free and democratic society. Stemming from the case *R. v. Oakes*, 1986 CanLII 46 (SCC), [1986] 1 SCR 103, this became known widely as the Oakes test. It requires:

- **Necessity:** there must be a clearly defined necessity for the use of the measure, in relation to a pressing societal concern (in other words, some substantial, imminent problem that the security measure seeks to treat).
- **Proportionality:** that the measure (or specific execution of an invasive power) be carefully targeted and suitably tailored, so as to be viewed as reasonably proportionate to the privacy (or any other rights) of the individual being curtailed.
- **Effectiveness:** that the measure be shown to be empirically effective at treating the issue, and so clearly connected to solving the problem.
- **Minimal intrusiveness:** that the measure be the least invasive alternative available (in other words, ensure that all other less intrusive avenues of investigation have been exhausted).[60]

---

[58] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-10. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_6.pdf. Accessed on June 12, 2020.
[59] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-10. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_6.pdf. Accessed on June 12, 2020.
[60] Privacy Commissioner of Canada, *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century* available at https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_sec_201011/. Accessed on June 12, 2020. See also SK OIPC Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on questions, screening or testing by employers regarding COVID-19. Available at https://oipc.sk.ca/advisory-from-the-office-of-the-

Local authorities should consider the following four-part test when considering new initiatives (e.g., services, programs, activities, proposed legislation, etc.) that impact privacy as early as possible in the development process:

(i) Is the measure demonstrably necessary to meet a specific need

(ii) Is it likely to be effective in meeting that need

(iii) Is the loss of privacy proportional to the benefit gained

(iv) Is there a less privacy intrusive way of achieving the same end[61]

Consent Requirements

LA FOIP is not consent based. Local authorities require a vast amount of personal information from citizens to provide the services that those citizens expect. This includes the operation of schools, hospitals, social services, and countless other services. To require express consent every time a local authority collected, used, or disclosed personal information would likely be unwieldy, inefficient, and cumbersome, not to mention expensive.[62]

However, there are provisions in LA FOIP that require the express consent of individuals for the collection, use and disclosure of personal information. The specific provisions that require express consent for collection, use and disclosure of personal information are as follows:

- Section 27 – individual consents to "use" of personal information
- Subsection 28(1) – individual consents to "disclosure" of personal information

Consent is generally conceived as the free and voluntary act of a sovereign individual. Consent needs to be thought of as a process that provides the individual with a measure of

---

information-and-privacy-commissioner-of-saskatchewan-on-questions-screening-or-testing-by-employers-regarding-covid-19/. Accessed June 12, 2020.

[61] Privacy Commissioner of Canada resource, *Data at Your Fingertips Biometrics and the Challenge to Privacy*. Available at https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-10. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_6.pdf. Accessed on June 12, 2020.

[62] SK OIPC Investigation Report F-2010-001 at [43].

control over their own personal information. Consent normally can be modified and can be revoked.[63]

Consent means voluntary agreement by a person in the possession and exercise of sufficient mental capacity to make an intelligent choice to do something proposed by another; it supposes a physical power to act, a moral power of acting and a serious, determined, and free use of these powers.[64]

Express consent is the highest standard and can be written (e.g., form or letter) or verbal.[65] It must be informed and meet all the criteria set out in section 11 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* (LA FOIP Regulations*)*. Express consent of the data subject usually cures what would otherwise be a privacy breach when certain personal information is collected, used, or disclosed.[66]

Consent must be obtained from an individual in a meaningful way. Where LA FOIP requires express consent, section 11 of the LA FOIP Regulations is engaged and sets out the manner in which consent should be acquired:

> **11**(1) If consent is required by the Act for the collection, use or disclosure of personal information, the consent:
>
> (a) must relate to the purpose for which the information is required;
> (b) must be informed;
> (c) must be given voluntarily; and
> (d) must not be obtained through misrepresentation, fraud or coercion.
>
> (2) A consent to the collection, use or disclosure of personal information is informed if the individual who gives the consent is provided with the information that a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure of personal information.
>
> (3) A consent may be given that is effective for a limited period.

---

[63] SK OIPC Investigation Reports F-2010-001 at [44] and F-2013-002 at [33].
[64] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[65] Government of Alberta, *Protecting Personal Information, A Workbook for Non-Profit Organizations, Discussion Draft, March 2010*. Available at Protecting Personal Information: A Workbook for Non-Profit Organizations (alberta.ca) at p. 9.
[66] SK OIPC Investigation Report F-2010-001 at [39].

(4) A consent may be express or implied unless otherwise provided.

(5) An express consent need not be in writing.

(6) A local authority, other than the local authority that obtained the consent, may act in accordance with an express consent in writing or a record of an express consent having been given without verifying that the consent meets the requirements of subsection (1) unless the local authority that intends to act has reason to believe that the consent does not meet those requirements

Section 11 of the LA FOIP Regulations provides that where consent is required in LA FOIP, that it be "informed" (see s. 11(1)(b) above).

Informed consent is where a person's agreement to allow something to happen is based on a full disclosure of facts needed to make the decision intelligently, i.e., knowledge of risks involved, alternatives, etc.[67]

Informed consent becomes extremely relevant when considering the notion of control over one's personal information. Unfortunately, many local authorities fall short when informing individuals of the potential collections, uses and/or disclosures of personal information. Often it is because of a lack of proper training of staff, a shortage of time or a misguided focus on making things more convenient for the local authority at the expense of the individual. As a result, the need to properly inform individuals is lost or forgotten. However, some of the benefits to the individual and the organization when proper informed consent is achieved include:

- Empowerment of the individual.
- Improved confidence and satisfaction with the organization.
- Avoids later misunderstandings and conflict between the organization and the individual.
- Compliance with the law.

Consent must be obtained from the individual in a meaningful way. For example, it is not enough to seek verbal or written consent if no information is provided regarding what the

[67] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

consent is needed for. When gathering express informed consent, local authorities can follow the following best practices:

1. **Ensure individuals know why their personal information is being collected.** To be informed, the explanations given to individuals should be clear and complete. Stating that the information is being collected for 'research purposes' or 'to process a claim' would be too vague and not specific enough.

2. **Ensure individuals know how their personal information will be used.** Individuals should be fully informed of all the ways the organization intends to use their personal information. Incomplete and vague explanations leave individuals without the proper knowledge to consent. In addition, long written explanations (more than 1 page) that use highly technical language make it less likely that individuals will read it or understand it. Make it 'user friendly'. Consider providing information, brochures or fact sheets that can be taken home by individuals that outline the potential purposes of collection and uses of the information.

3. **Ensure that individuals know that they have the right to refuse or revoke their consent.** Consent from individuals must be given freely and without threat or coercion. The threat of not receiving a necessary service, if consent is not given, interferes with an individual's right to refuse or revoke their consent. Employees should be aware of when consent is required to deliver a service so they can properly inform individuals of the consequences of not providing consent. Some services can still be provided without the full collection and use of personal information. Employees require clarity on what is essential and what is not. Consider developing policies and procedures to guide employees in this regard.

4. **Ensure your organization has clear policies and procedures regarding the collection, use or disclosure of personal information with appropriate enforcement policies.** Improper behavior on the part of employees is not uncommon when it comes to the use of consent forms. Organizations should ensure its employees do not pressure, coerce or threaten individuals into agreeing to sign consent forms. Consider training, written policies and procedures and enforcement mechanisms.[68]

---

[68] SK OIPC resource, *Best Practices for Gathering Informed Consent and the Content of Consent Forms* available at Best Practices for Gathering Informed Consent and the Content of Consent Forms (oipc.sk.ca) at p. 2.

Meaningful consent means that an individual is empowered to make an informed decision about whether they wish to provide their consent or not when it comes to the collection, use and disclosure of their personal information.

Best Practice Steps for Consent Forms

The following information has been reproduced from IPC resource, *Best Practices for Gathering Informed Consent and the Content of Consent Forms* available at https://oipc.sk.ca. For more detailed information, please refer to that resource.

The following are some best practices for the content of consent forms:

1. **Ensure consent forms are time limited**. Consent is not intended to be indefinite for the collection, use and/or disclosure of personal information. Consent forms should have a beginning and end date which covers the amount of time that the consent remains valid and is actually needed by the organization. Research has shown that consent forms with definite expiration dates (6 months or less) are more likely to be signed by individuals. They are less likely to be comfortable signing it if the expiration is ambiguous.[69]

2. **Ensure consent forms are information specific (data minimization /avoid over-collection).** The consent form should outline the specific types of personal information that is being collected, used and/or disclosed. This assists in reducing risks such as over-collection. Organizations should collect, use and/or disclose the least amount of personal information necessary for the purpose. To ensure this, organizations should know prior to the collection, use and/or disclosure what is needed. For example, if an individual's medical information is needed, the consent form should be specific as to what type of information is being collected, used and/or disclosed. Rather than "the entire medical record" it could state "only psychological assessments, physical assessments and medication history".

3. **Consent forms should be signed by both the individual and the employee presenting the consent form**. To ensure authenticity, consent forms should be signed by both parties to the consent form. It is important that the employee of the organization also sign as they are responsible for having properly acquired the consent should problems arise. This, of course, would need to be adapted for consent forms received

[69] Bolcic-Jankovic, Dragana et al. 2007. "*Do Characteristics of Consent Forms Affect the Response Rate?*" Center for Survey Research, University of Massachusetts: Boston.

electronically. There should be one consent form for each person whose personal information is involved.

4. **Consent forms should include the specific names of the involved parties that will be collecting or disclosing the personal information (need-to-know principle)**. Consent forms should have the name of the sending party and the name of the party that will receive it. This ensures that the scope of the collection and disclosure is limited to the individuals identified.

Section 23: Definition of Personal Information

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

(a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;

(b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) information that relates to health care that has been received by the individual or to the health history of the individual;

(d) any identifying number, symbol or other particular assigned to the individual;

(e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;

(f) the personal opinions or views of the individual except where they are about another individual;

(g) correspondence sent to a local authority by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;

(h) the views or opinions of another individual with respect to the individual;

(i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;

Office of the Saskatchewan Information and Privacy Commissioner. Guide to LA FOIP, Chapter 6, *Protection of Privacy*. Updated 27 February 2023.

(j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or

(k) the name of the individual where:

(i) it appears with other personal information that relates to the individual; or

(ii) the disclosure of the name itself would reveal personal information about the individual.

(1.1) On and after the coming into force of subsections 4(3) and (6) of *The Health Information Protection* Act, with respect to a local authority that is a trustee as defined in that Act, **"personal information"** does not include information that constitutes personal health information as defined in that Act.

(1.2) Personal health information in the possession or control of the Workers' Compensation Board is personal information for the purposes of this Act.

(2) **"Personal information"** does not include information that discloses:

(a) the classification, salary, discretionary benefits or employment responsibilities of an individual who is or was an officer or employee of a local authority;

(b) the personal opinions or views of an individual employed by a local authority given in the course of employment, other than personal opinions or views with respect to another individual;

(c) financial or other details of a contract for personal services;

(d) details of a licence, permit or other similar discretionary benefit granted to an individual by a local authority;

(e) details of a discretionary benefit of a financial nature granted to an individual by a local authority;

(f) expenses incurred by an individual travelling at the expense of a local authority;

(g) the academic ranks or departmental designations of members of the faculties of the University of Saskatchewan or the University of Regina; or

(h) the degrees, certificates or diplomas received by individuals from the Saskatchewan Polytechnic, the University of Saskatchewan or the University of Regina.

(3) Notwithstanding clauses (2)(d) and (e), **"personal information"** includes information that:

(a) is supplied by an individual to support an application for a discretionary benefit; and

(b) is personal information within the meaning of subsection (1).

For the privacy provisions at Part IV of LA FOIP to be engaged, the information at issue must constitute "personal information".

Office of the Saskatchewan Information and Privacy Commissioner. Guide to LA FOIP, Chapter 6, *Protection of Privacy*. Updated 27 February 2023.

Subsection 23(1) of LA FOIP starts with the following:

> **23**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
> …

The list of examples provided for at subsection 23(1) of LA FOIP is not meant to be exhaustive. This means there can be other types of information that could qualify as personal information.

Including means that the list of information that follows is incomplete (non-exhaustive). The examples in the provision are the types of information that could be presumed to qualify as personal information.[70]

However, more broadly, to constitute personal information, two elements must be present:

1. The information must be about an identifiable individual; and

2. The information must be personal in nature.

1. Is the information about an identifiable individual?

Information is about an identifiable individual if:

- The individual can be identified from the information (e.g., name, where they live); or
- The information, when combined with information otherwise available, could reasonably be expected to allow the individual to be identified.[71]

---

[70] British Columbia Government Services, *FOIPPA Policy and Procedures Manual* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/cabinet-local-public-body-confidences. Accessed June 26, 2019. Definition of "including" as included in SK OIPC *Guide to LA FOIP*, *Chapter 4 – Exemptions from the Right of Access*, for subsection 16(1)(e) of FOIP.

[71] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 2, Scope of FIPPA – Who and What Falls under FIPPA* at p. 44. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_2.pdf. Accessed on April 24, 2020.

About means on the subject of or concerning.[72] *About* an identifiable individual means the information is not just the subject of something but also relates to or concerns the subject.[73]

Identifiable means that it must be reasonable to expect that an individual may be identified if the information were disclosed.[74] The information must reasonably be capable of identifying particular individuals because it either directly identifies a person or enables an accurate inference to be made as to their identity when combined with other available sources of information (data linking) or due to the context of the information in the record.[75]

LA FOIP uses the terms "person" and "individual" and each term has different meanings. "*Person*" is the broader term and means individual but also includes a corporation and their heirs, executors, administrators, or other legal representatives of a person.[76]

Individual means natural persons (human beings).[77] Use of the word *individual* in this provision makes it clear that the protection provided relates only to a natural person or human being.[78]

IPC Findings

In Review Report LA-2014-002, the Commissioner found that a severed portion of handwritten notes consisting of two words and one symbol did not link to an identifiable

---

[72] Pearsall, Judy, *Concise Oxford Dictionary, 10th Ed.*, (Oxford University Press) at p. 4.
[73] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII), [2007] 1 FCR 203. Also see the Office of the Privacy Commissioner of Canada resource, *PIPEDA Interpretation Bulletin: Personal Information*, 2013, available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/.
[74] ON IPC Order PO-1880, upheld on judicial review in *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300 (C.A.). See also SK OIPC Review Report LA-2013-001 at [57].
[75] Originated and adapted from Office of the British Columbia Information and Privacy Commissioner (BC IPC) Order P14-03 at [16].
[76] *The Legislation Act*, SS 2019, c L-10.2 at s. 2-29.
[77] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at pp. 924, 1238 and 1378.
[78] ON IPC Order 16 at p. 19. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 2, Scope of FIPPA – Who and What Falls under FIPPA* at p. 44. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_2.pdf. Accessed on April 24, 2020.

individual. Accordingly, the Commissioner found insufficient evidence it constituted personal information and recommended this portion be released.

2. Is the information personal in nature?

Use of the word "*personal*" as the adjective to describe the type of information being considered in subsection 23(1) of LA FOIP is a clear indication that the Legislature intended for the provision to cover information that is "*personal*" in nature. To ignore this would be to fail to follow the modern approach to statutory interpretation. In *John Doe v. Ontario (Finance*), [2014] 2 SCR 3, 2014 SCC 36 (CanLII), the court reiterated that the modern approach requires that words be "read in their entire context, according to their grammatical and ordinary sense, harmoniously with the scheme and object of the Act and the intention of the legislature".[79]

Personal in nature requires that the information reveal something personal about the identifiable individual.[80]

Personal means of, affecting or belonging to a particular person; of or concerning a person's private rather than professional life.[81]

Therefore, information that relates to an individual in a professional, official, or business capacity could only qualify if the information revealed something personal about the individual for example, information that fits the definition of employment history.[82]

The Ontario Information and Privacy Commissioner's office asks the following questions:

- *In what context do the names of individuals appear?* Is it a context that is inherently personal, or is it one such as a business, professional or government context that is removed from the personal sphere?
- *Is there something about the information at issue that, if disclosed, would reveal something of a personal nature about the individual?* Even if information appears in a

[79] SK OIPC Review Report 082-2019, 083-2019 at [93].
[80] ON IPC Orders R-980015 at p. 17, PO-2420 at p. 3 and PO-2060 at p. 2. First relied on in SK OIPC Review Report F-2010-001 at [126].
[81] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 1065, (Oxford University Press).
[82] Originated from ON IPC Orders P-257, P-427, P-1412, P-1621, R-980015, MO-1550-F, PO-2225, P-1409, PO-2420 and PO-2271. See also SK OIPC Review Report F-2010-001 at [126].

business context, would its disclosure reveal something that is inherently personal in nature?[83]

Recorded in any form means that the personal information must be on a record for Part IV of LA FOIP to be engaged. If it is not in recorded form, it does not qualify as personal information for purposes of LA FOIP.[84] Where a local authority verbally discloses personal information, if the information was recorded somewhere, the disclosure rules of LA FOIP still apply.[85] In other words, if the information exists or existed at one time in recorded format, LA FOIP will apply. To determine otherwise would facilitate the circumvention of the non-disclosure rules contained in Part IV and would be inconsistent with the purposes of the Act.[86]

Record means a record of information in any form and includes information that is written, photographed, recorded, or stored in any manner, but does not include computer programs and other mechanisms that produce records.[87]

Subjective information is information based on or influenced by personal feelings, tastes, or opinions.[88] Subjective information about an individual may still be personal information even if it is not necessarily accurate.[89]

What is not Personal Information?

The IPC has consistently found that certain information does not qualify as personal information in several reports. This information includes:

---

[83] The ON IPC utilizes this approach. See ON IPC Orders PO-3180 at p. 8, PO-2225 at p. 7, PO-3148 at [80], MO-2342 at p. 4 and PO-2934 at p. 6.
[84] SK OIPC Investigation Report 127-2017 at [9] and [11]. Unlike FOIP, *The Health Information Protection Act* (HIPA) does not carry the requirement that information must be in recorded form.
[85] SK OIPC Investigation Report 105-2014 at [46].
[86] BC IPC Order F14-26 at [16]. Similar position taken by ON IPC in Privacy Complaint No. MC-020008-1 at p. 2.
[87] *The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c L-27.1 at subsection 2(i).
[88] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 1427, (Oxford University Press).
[89] Office of the Privacy Commissioner of Canada resource, *PIPEDA Interpretation Bulletin: Personal Information*, 2013, available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/.

Work product is information generated by or otherwise associated with an individual in the normal course of performing his or her professional or employment responsibilities, whether in a public or private setting. This is not considered personal information.[90]

Business card information is the type of information found on a business card (name, job title, work address, work telephone numbers and work email address). This type of information is generally not personal in nature and therefore would not be considered personal information. This is considered "*business contact information*" and not personal information.[91]

Employer assigned cell phone numbers are considered business card information. This interpretation has been applied to business cell phone numbers for local authority employees, non-local authority employees, professionals, and corporate officers.[92]

A name alone is not personal information unless release of the name itself would reveal personal information about the individual.[93]

Names of nurses and firefighters were found to not be personal information.[94]

Signatures when made in a work-related capacity were found to not be personal information. However, a signature may be personal in nature outside of the professional context.[95]

Information relating to the position, function or responsibilities of an individual pertain more to a job description of an individual and are not personal in nature. This includes terms and conditions associated with a particular position, including such information as qualifications, duties, responsibilities, hours of work and salary range.[96] Sign-in logs

---

[90] First cited in SK OIPC Review Report F-2006-001 at [113]. See also SK OIPC *2012-2013 Annual Report* at p. 12. See also BC IPC Order P14-03 at [17] to [18].
[91] First cited in SK OIPC Review Report F-2010-001 at [124]. See also SK OIPC *2012-2013 Annual Report* at p. 12. See also ON IPC Order P-1409 at p. 24.
[92] See SK OIPC Review Report 277-2016 at [41].
[93] See subsection 23(1)(k)(ii) of LA FOIP. First cited in SK OIPC Review Report 2003-014 at [26]. Later referenced in SK OIPC Review Report F-2005-001 at [13]. See also SK OIPC Review Reports F-2012-006 at [147], F-2014-005 at [10], 195-2015 and 196-2015 at [17] and 112-2018 at [46]. See also *General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance*, 1993 CanLII 9128 (SK CA) at [14] and *Griffiths v. Nova Scotia (Education)*, 2007 NSSC 178 (CanLII) at [24].
[94] See SK OIPC Review Reports LA-2012-002 at [26] and F-2006-001 at [113].
[95] See SK OIPC Review Report 156-2015 at [6].
[96] See SK OIPC Review Report LA-2012-002 at [25].

containing the name, dates and times individuals went to their workplaces is about the position and is not personal information.[97]

The rationale for a distinction between personal information and information that relates to a person in their professional or official capacity preserves the integrity of the regime that establishes the public's right of access and a local authority's disclosure obligations. Without this distinction, the routine disclosure of information by local authorities would be greatly impeded. For example, withholding all recorded information relating to the activities of public servants or other individuals in their professional or official capacities impedes LA FOIP's overarching goal of creating accountability and transparency over local authority activities. Further, not differentiating between information that is personal in nature and information that relates to a person's professional capacity would frustrate the purpose of LA FOIP, namely that information under the possession or control of a local authority should be made available to the public (unless subject to a limited and specific exemption).[98]

IPC Findings

In Review Report 277-2016, the Commissioner found that employer assigned cell phone numbers for government employees was considered business card information and not personal information. Further, the Commissioner found that the same approach is taken to business cell phone numbers of non-government employees, professionals and corporate officers.

In Review Reports LA-2012-002, F-2006-001 and 277-2016, the Commissioner found that the names of nurses, firefighters and lawyers were not personal information.

In Review Report LA-2012-002, the Commissioner found that a position, function, responsibilities and hours of work pertained more to a job description than personal information of the individual.

In *Dagg v. Canada (Minister of Finance) (1997)*, the court decided that sign-in logs containing the names, dates and times individuals went to their workplaces constituted information about the positions and not information that was personal in nature of the employees.

In Review Reports LA-2014-002, 156-2015 and Investigation Report 059-2018, the Commissioner found that signatures provided in a work-related capacity did not constitute

[97] *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC), [1997] 2 SCR 403 at [95].
[98] Adapted from ON IPC Reconsideration Order R-980015 at pp. 9 and 10.

personal information. However, a signature may be personal in nature and qualify as personal information if made outside of a professional context.

In Investigation Report 070-2018, the Commissioner found that the name of a landlord, the landlord's advertisement seeking a new tenant and the fact that a previous tenant had vacated was not personal information. This finding was because the landlord was functioning in a professional or business capacity and the advertisement did not contain anyone's personal information. Further, the landlord's property being vacated was not the personal information of the landlord but rather information about the rental property.

Subsection 23(1)(a)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

(a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;

Subsection 23(1)(a) of LA FOIP defines certain information as personal information. This includes:

Race means culturally or socially constructed divisions of humankind, based on distinct characteristics that can be based on physicality, culture, history, beliefs and practices, language, origin, etc.[99] It has also been defined as each of the major divisions of humankind, having distinct physical characteristics, racial origin, or distinction.[100] An example of race is brown, white, or black skin (all from various parts of the world). Racial origin means the identification of the common descent that connects a group of persons. The Mongolian race and the Caucasian race are examples. An example in a record would be a letter on file of a client of a ministry that makes note of the fact that a client is eligible for specific benefits as an aboriginal person.[101]

---

[99] The 519, Education and Training, Glossary of Terms, available at https://www.the519.org/education-training/glossary#. Accessed April 22, 2020.
[100] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 1178, (Oxford University Press).
[101] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Creed refers to an individual's basic beliefs of a religion or an idea or set of beliefs that guide the actions of a person.[102] The following characteristics are relevant when considering if a belief system is a creed. A creed:

- Is sincerely, freely, and deeply held
- Is integrally linked to a person's identity, self-definition, and fulfilment
- Is a particular and comprehensive, overarching system of belief that governs one's conduct and practices
- Addresses ultimate questions of human existence, including ideas about life, purpose, death, and the existence or non-existence of a Creator and/or a higher or different order of existence
- Has some "nexus" or connection to an organization or community that professes a shared system of belief[103]

Religion includes all aspects of religious observance and practice as well as beliefs.[104]

Colour means pigmentation of the skin, especially as an indication of someone's race.[105] Colour includes, for example, being black or white.[106]

'Sex' and 'gender' are often used interchangeably, despite having different meanings:

> **Sex** refers to a set of biological attributes in humans and animals. It is primarily associated with physical and physiological features including chromosomes, gene expression, hormone levels and function, and reproductive/sexual anatomy. Sex is usually categorized as female or male but there is variation in the biological attributes that comprise sex and how those attributes are expressed.[107] It has also been defined as the classification of people as either male, female, or intersex.[108]

---

[102] "Creed." *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/creed. Accessed April 23, 2020.
[103] Ontario Human Rights Commission, *Policy on preventing discrimination based on creed*, available at http://www.ohrc.on.ca/en/policy-preventing-discrimination-based-creed. Accessed April 21, 2020.
[104] *The Saskatchewan Human Rights Code, 2018*, SS 2018, c S-24.2 at s. 2(1).
[105] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 282, (Oxford University Press).
[106] University of Cambridge, *Equality & Diversity, Race,* available at https://www.equality.admin.cam.ac.uk/training/equalities-law/protected-characteristics/race. Accessed April 22, 2020.
[107] Canadian Institutes of Health Research, *What is gender? What is sex?* Available at What is gender? What is sex? - CIHR (cihr-irsc.gc.ca). Accessed on October 25, 2022.
[108] The 519, Education and Training, Glossary of Terms, available at https://www.the519.org/education-training/glossary#. Accessed April 22, 2020.

Gender refers to the socially constructed roles, behaviors, expressions and identities of girls, women, boys, men, and gender diverse people. It influences how people perceive themselves and each other, how they act and interact, and the distribution of power and resources in society. Gender identity is not confined to a binary (girl/woman, boy/man) nor is it static; it exists along a continuum and can change over time. There is considerable diversity in how individuals and groups understand, experience and express gender through the roles they take on, the expectations placed on them, relations with others and the complex ways that gender is institutionalized in society.[109] A person may identify with genders that are different from their sex or with none at all. These identities may include transgender, nonbinary, or gender neutral.

Sexual orientation means the direction of one's attraction. Some people use the terms gay, straight, bisexual, pansexual, or lesbian to describe their experience.[110]

Family status means the status of being in a parent and child relationship. For the purposes of this definition:

> **child** means son, daughter, stepson, stepdaughter, adopted child and a person to whom another person stands in place of a parent.
>
> **parent** means father, mother, stepfather, stepmother, adoptive parent, and person who stands in place of a parent to another person.[111]

Marital status means the status of being engaged to be married, married, single, separated, divorced, widowed, or living in a common-law relationship.[112]

Disability means:

(a) any degree of physical disability, infirmity, malformation, or disfigurement, including:
  (i) epilepsy;
  (ii) any degree of paralysis;
  (iii) amputation;
  (iv) lack of physical coordination;
  (v) blindness or visual impediment;

---

[109] Canadian Institutes of Health Research, *What is gender? What is sex?* Available at What is gender? What is sex? - CIHR (cihr-irsc.gc.ca). Accessed on October 25, 2022.
[110]The 519, Education and Training, Glossary of Terms, available at https://www.the519.org/education-training/glossary#. Accessed April 22, 2020.
[111] *The Saskatchewan Human Rights Code, 2018*, SS 2018, c S-24.2 at s. 2(1). See also SK OIPC Review Report 109-2015 at [40].
[112] *The Saskatchewan Human Rights Code, 2018*, SS 2018, c S-24.2 at s. 2(1).

(vi) deafness or hearing impediment;
(vii) muteness or speech impediment; or
(viii) physical reliance on a service animal, wheelchair or other remedial applicant or device; or

(b) any of the following disabilities:
(i) an intellectual disability or impairment;
(ii) a learning disability, or a dysfunction in one or more of the processes involved in the comprehension or use of symbols or spoken language;
(iii) a mental disorder;[113]

Age means the length of time that a person has existed.[114]

Nationality means the status of belonging to a particular nation; an ethnic group forming a part of one or more political nations.[115] The relationship between a citizen of a country and the country itself; membership in a country.[116] It includes, for example, being a British, Jamaican, or Pakistani citizen.[117]

Ancestry means a person's ancestors or ethnic descent.[118]

Place or origin means birthplace or nativity.[119] The place where a person was born.

IPC Findings

In Investigation Report F-2012-004, the Commissioner found that an individual's "*age*" qualified as personal information pursuant to the equivalent subsection 24(1)(a) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

[113] *The Saskatchewan Human Rights Code, 2018*, SS 2018, c S-24.2 at s. 2(1).
[114] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 24, (Oxford University Press).
[115] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 949, (Oxford University Press).
[116] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1234.
[117] University of Cambridge, Equality & Diversity, Race, available at https://www.equality.admin.cam.ac.uk/training/equalities-law/protected-characteristics/race. Accessed April 22, 2020.
[118] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 48, (Oxford University Press).
[119] "Birthplace" in Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 138, (Oxford University Press). See also "Nativity." *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/nativity. Accessed April 23, 2020.

In Investigation Report F-2014-002, the Commissioner found that the number of nephews the Complainant had constituted personal information of the Complainant pursuant to the equivalent subsection 24(1)(a) of FOIP. The number of nephews reveals "*family status*".

In Review Report 138-2015, the Commissioner found that the faces of individuals in video surveillance recordings (except government employees and Saskatoon Police Service members) constituted personal information pursuant to the equivalent subsection 24(1)(a) of FOIP. An image of an individual's face could reveal "*race*", "*colour*", "*sex*" or "*disability*".

In Investigation Report 189-2015, the Commissioner found that the date of birth of an individual qualified as personal information pursuant to the equivalent subsection 24(1)(a) of FOIP. A birth date reveals the "*age*" of an individual.

In Investigation Report 219-2015, the Commissioner found that the fact a Power of Attorney between a Complainant and their son was listed on a meeting agenda qualified as personal information pursuant to the equivalent subsection 24(1)(a) of FOIP.

Subsection 23(1)(b)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

Education history refers to any information regarding an individual's schooling. This includes names of schools, colleges or universities attended, courses taken, and grades achieved. For example, an individual's high school grade point average, individual assignment marks and/or course marks.[120]

[120] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020. See also Government of Newfoundland and Labrador ATIPP Office, *Access to Information Policy and Procedures Manual*,

To qualify as employment or educational history, the information must contain some significant part of the history of the person's employment or education. For example, a student's course enrolment and academic performance. An example of what would not be significant enough includes records that simply list student names and generic attendance information not associated to any particular student and reveals only the fact that a student attended a certain school during a brief point in time.[121]

Criminal history includes an individual's convictions under criminal laws such as the *Criminal Code* (Canada) and findings of guilt under the *Youth Criminal Justice Act* (Canada) or the former *Young Offenders Act* (Canada). Other offences include "*Regulatory offences*" such as:

- Offences under other federal statutes or regulations (for example, the *Immigration and Refugee Protection Act* (Canada));
- Offences under provincial statutes or regulations (for example, *The Traffic Safety Act* (Saskatchewan); or
- Offences under municipal by-laws.[122]

Employment history is the type of information normally found in a personnel file such as performance reviews, evaluations, disciplinary actions taken, reasons for leaving a job, information in a résumé or leave transactions.[123]

It does not include work product.[124] General information, such as references to the type of employment entered into, certain actions taken, and relevant dates of those options are also not included.[125]

Employment history does not include:

October 2017 at p. 100 and Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 32. Adopted in SK OIPC Investigation Report LA-2013-003 at [25].

[121] ON IPC Order MO-3900 at [46] to [48].

[122] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 2, Scope of FIPPA – Who and What Falls under FIPPA* at p. 44. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_2.pdf. Accessed on April 24, 2020.

[123] Office of the Information and Privacy Commissioner of Alberta (AB IPC) Order F2003-005 at [73]. Similar view taken by ON IPC in Order M-615 at p. 4 and Office of the Prince Edward Island Information and Privacy Commissioner (PEI IPC) Order No. 07-001 at p. 17. First adopted by SK OIPC in Review Report LA-2009-002/H2009-001 at [170] to [174].

[124] First cited in SK OIPC Review Report F-2006-001 at [113]. See *What is not personal information* section above in this Chapter for definition of "work product".

[125] AB IPC Order F2003-005 at [73]. See also ON IPC in Order M-615 at p. 4.

- Discreet pieces of information that might reveal information about a particular episode in a person's employment (e.g., names of employees interviewed with respect to a complaint). Employment history does not include every action of an individual employee. The fact that a named public servant has performed or undertaken a specific task is not "employment history" in the requisite sense.
- Employment history refers only to past employment and not to aspects of current employment such as an employee's current salary or job position.
- It does not include a person's name, without more.
- It does not generically refer to all employment-related incidents.[126]

The mere fact that an individual is granted an interview for a position does not constitute that person's employment history.[127]

Financial transactions are not defined in LA FOIP. However, the definition can be broken down as follows:

> **Financial** means of or pertaining to revenue or money matters.[128]
>
> **Transaction** means something performed or carried out; a business agreement or exchange; any activity involving two or more persons.[129]

Relating to should be given a plain but expansive meaning.[130] The phrase should be read in its grammatical and ordinary sense. There is no need to incorporate complex requirements (such as "substantial connection") for its application, which would be inconsistent with the plain unambiguous meaning of the words of the statute.[131] "*Relating to*" requires some connection between the information and the financial information.[132]

---

[126] ON IPC Reconsideration Order R-980015 at pp. 16 and 17. Also cited in SK OIPC Review Report LA-2013-001 at [95].
[127] ON IPC Order P-485 at p. 4.
[128] *The Shorter Oxford English Dictionary on Historical Principles*, Oxford University Press 1973, Volume 1 at p. 964.
[129] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1802.
[130] *Gertner v. Lawyers' Professional Indemnity Company,* 2011 ONSC 6121 (CanLII) at [32].
[131] *Ministry of Attorney General and Toronto Star*, 2010 ONSC 991 (CanLII) at [45]. This case dealt specifically with an appeal regarding Ontario's FOIP legislation.
[132] Adapted from *Ministry of Attorney General and Toronto Star*, 2010 ONSC 991 (CanLII) at [43].

IPC Findings

In Investigation Report F-2012-004, the Commissioner found that an employee number, hire date, last date worked, re-hire date and action to be taken regarding an individual's employment status would qualify as "*employment history*" and constituted personal information pursuant to the equivalent subsection 24(1)(b) of *The Freedom of Information and Protection of Privacy Act* (FOIP). Further, the Commissioner found that pay type, pay rate, annual earnings, standard hours per pay would constitute "*financial transactions*" in which the individual was involved and qualified as personal information pursuant to the equivalent subsection 24(1)(b) of FOIP.

In Investigation Report F-2014-002, the Commissioner found that the fact a complainant had paid certain individuals qualified as "*financial transactions*" the complainant was involved in and constituted personal information pursuant to the equivalent subsection 24(1)(b) of FOIP.

In Review Report 146-2017, the Commissioner found that whether or not an individual passed or failed an online exam qualified as "*educational history*" and constituted personal information pursuant to the equivalent subsection 24(1)(b) of FOIP.

Subsection 23(1)(c)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(c) information that relates to health care that has been received by the individual or to the health history of the individual;

This provision is unique to LA FOIP and does not appear in *The Freedom of Information and Protection of Privacy Act* (FOIP). The reason for this is to ensure privacy protection for certain personal health information in the possession or control of a local authority where the local authority is not also a trustee under *The Health Information Protection Act* (HIPA).

To clarify further, all government institutions under FOIP also qualify as trustees under HIPA (see s. 2(t)(i) of HIPA). Conversely, not all local authorities qualify as trustees under HIPA.

Some local authorities also qualify as trustees under HIPA. For example, the Saskatchewan Health Authority is both a local authority under subsection 2(f)(xiii) of LA FOIP and also a trustee pursuant to subsection 2(t)(ii) of HIPA. For personal health information in the possession/custody or control of local authorities that are also trustees, HIPA applies to that personal health information and not LA FOIP (as per s. 4(3) of HIPA which states HIPA applies to personal health information and not LA FOIP).

However, for local authorities that are not also trustees, LA FOIP would apply to certain personal health information described in LA FOIP (like subsection 23(1)(c) of LA FOIP). For example, the Regina Police Service is a local authority under subsection 2(f)(viii.1) of LA FOIP but is not a trustee under subsection 2(t) of HIPA. Therefore, provisions like subsection 23(1)(c) of LA FOIP would be engaged to protect personal health information collected, used or disclosed by the RPS in the carrying out of its work. The personal health information is treated like "personal information" under LA FOIP.

Without provisions like subsection 23(1)(c) of LA FOIP, some of the personal health information in the possession or control of local authorities that are not also trustees would not have privacy protection.

It is important to clarify, that where an organization qualifies as both a local authority and a trustee, LA FOIP does not apply to personal health information in the possession or control of the local authority. Rather, HIPA applies to that information. This is supported by subsection 23(1.1) of LA FOIP and subsections 4(3) and 4(6) of HIPA. See *Subsection 23(1.1)* later in this Chapter for more on the interpretation of subsection 23(1.1) of LA FOIP.

To summarize how to approach personal health information in the possession or control of a local authority:

- If the local authority is also a trustee, HIPA should be relied on for the rules and protection of personal health information.
- If the local authority is not also a trustee, LA FOIP should be relied on (only as provided for in LA FOIP) for the rules and protection of personal health information.

Subsection 23(1)(c) of LA FOIP provides that information that relates to health care that has been received or the health history of an individual qualifies as "personal information" for purposes of LA FOIP.

Relates to should be given a plain but expansive meaning.[133] The phrase should be read in its grammatical and ordinary sense. There is no need to incorporate complex requirements (such as "substantial connection") for its application, which would be inconsistent with the plain unambiguous meaning of the words of the statute.[134] "*Relating to*" requires some connection between the information and health care received or the health history of the individual.[135]

Health care means collectively, the services provided, usually by medical professionals, to maintain and restore health.[136]

Health history means a record of information about a person's health. A personal history may include information about allergies, illnesses, surgeries, immunizations, and results of physical exams and tests. It may also include information about medicines taken and health habits, such as diet and exercise.[137]

IPC Findings

In Investigation Report 109-2017, the Commissioner investigated an alleged breach of privacy involving Englefeld Protestant Separate School Division #132 (Englefeld). The complaint alleged that Englefeld disclosed personal information to the Ministry of Social Services inappropriately. During the investigation, the Commissioner determined that information about the child's special needs and the requirement for supports at school qualified as the child's "health history" and was therefore personal information pursuant to subsection 23(1)(c) of LA FOIP.

In Investigation Report 002-2018, the Commissioner investigated an alleged breach of privacy involving Saskatchewan Polytechnic (SaskPolytech). A complainant alleged that her personal information was disclosed by SaskPolytech's legal counsel at an arbitration hearing involving a grievance and harassment allegations against a faculty member. According to the complaint, SaskPolytech disclosed personal information from a Medical Certificate Form from the complainant's personnel file during the arbitration during cross-examination. The

[133] *Gertner v. Lawyers' Professional Indemnity Company,* 2011 ONSC 6121 (CanLII) at [32].
[134] Adapted from *Ministry of Attorney General and Toronto Star*, 2010 ONSC 991 (CanLII) at [45].
[135] Adapted from *Ministry of Attorney General and Toronto Star*, 2010 ONSC 991 (CanLII) at [43].
[136] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 865.
[137] National Cancer Institute, *Definition of health history*. Available at Definition of health history - NCI Dictionary of Cancer Terms - NCI. Accessed on February 2, 2023.

Commissioner found that the information in the Medical Certificate Form qualified as personal information pursuant to subsection 23(1)(c) of LA FOIP.

In Review Report 243-2019, the Commissioner reviewed a denial of access to information involving the Rural Municipality of Blaine Lake No. 434 (RM). The RM had received an access to information request for all time sheets for a specific foreman during a specific timeframe. The RM withheld portions of the records from the applicant. During the review, the Commissioner determined that some of the information withheld on the timesheets appeared to refer to medical services received by a specific individual and therefore it qualified as that individual's personal information pursuant to subsection 23(1)(c) of LA FOIP. The Commissioner noted that this type of information should not be noted on timesheets, and it was an inappropriate collection of personal information. The RM acknowledged this fact and created a policy that clearly outlined what should and should not be found on a timesheet.

In Review Report 039-2020, the Commissioner reviewed a denial of access to information involving the Saskatoon Police Service (SPS). An applicant had requested access to notes and/or any reporting that was done in regard to the applicant's call to police on a specific date. SPS withheld some information. Upon review, the Commissioner determined that medical records and health information was withheld appropriately pursuant to subsection 23(1)(c) of LA FOIP. This included photographs documenting alleged injuries.

In Investigation Report 064-2022, 115-2022, the Commissioner investigated an alleged breach of privacy complaint involving the Saskatoon Public Library (SPL). The complaint alleged that SPL required the complainant to submit a rapid antigen test result every 72 hours, since they had not submitted proof of full COVID-19 vaccination. As part of the investigation, the Commissioner determined that the COVID-19 test results revealed the complainant's "health history" and would therefore qualify as personal information pursuant to subsection 23(1)(c) of LA FOIP.

Subsection 23(1)(d)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(d) any identifying number, symbol or other particular assigned to the individual;

An identifying number or symbol is, by itself, a piece of personal information because it uniquely identifies an individual. Examples include an individual's social insurance number, driver's licence number[138], passport number and client numbers assigned by a local authority or bank.[139]

Employee number when linked with a name was found to be personal information.[140]

Health services number means a unique number assigned to an individual who is or was registered as a beneficiary to receive insured services within the meaning of *The Saskatchewan Medical Care Insurance Act*.[141]

> Note: Subsection 23(1)(d) of LA FOIP would capture health services numbers in instances where the local authority is not also a trustee.
>
> If the local authority is also a trustee, the health services number would be "personal health information" and would be captured by *The Health Information Act* as per subsection 23(1.1) of LA FOIP. See *Subsection 23(1.1)* below in this Chapter for further assistance.

---

[138] History of SK OIPC approach: In Review Reports F-2013-007 at [125], 031-2015 at [44], 129-2015 at [33], 010-2016 at [25], 244-2017 at [17] and Investigation Report F-2012-001 at [6] and footnote [2], the Commissioner found a "driver's licence number" qualified as personal information pursuant to subsection 24(1)(d) of FOIP. In Review Reports 063-2017, 146-2017 and Investigation Report 096-2018, the Commissioner found that a "driver's licence number" was not personal information because of subsection 24(2)(e) of FOIP. In the 2018 decision, *Shook Legal, Ltd v Saskatchewan (Government Insurance)*, 2018 SKKB 238 (CanLII), it was found that the "*details of a licence*" as per subsection 24(2)(e) included name, address, description of the vehicle to be licenced and vehicle registration number (VIN) (see paragraph [34] of the decision). This is supported by the 1993 Saskatchewan Court of Appeal decision, *General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance*, 1993 CanLII 9128 (SK CA) which stated ""*Details of a licence or permit*" does not contemplate release of a core of personal data that one provides in confidence."

[139] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 2, Scope of FIPPA – Who and What Falls under FIPPA* at p. 52. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_2.pdf. Accessed on April 24, 2020.

[140] See SK OIPC F-2005-001 at [22] and LA-2012-002 at [29] to [30] and [106].

[141] Definition originates from *The Health Information Protection Act* at s. 2(i).

IPC Findings

In Investigation Reports F-2005-001 and LA-2012-002, the Commissioner found that *employee numbers* qualified as an "identifying number" and constituted personal information pursuant to the equivalent subsection 24(1)(d) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

In Investigation Report F-2012-004, the Commissioner found that *social insurance numbers* qualified as an "identifying number" and constituted personal information pursuant to the equivalent subsection 24(1)(d) of FOIP.

In Review Report F-2013-007, the Commissioner found that *claim numbers* qualified as an "identifying number" and constituted personal information pursuant to the equivalent subsection 24(1)(d) of FOIP.

In Review Report 031-2015, the Commissioner found that a *driver's licence number* qualified as a "identifying number" and constituted personal information pursuant to the equivalent subsection 24(1)(d) of FOIP.

In Review Report 117-2018, the Commissioner found that a company's *business number* (the nine-digit number Canada Revenue Agency assigns to a business) did not qualify as personal information, but rather third party information pursuant to subsection 19(1)(b) of FOIP (equivalent subsection 18(1)(b) in LA FOIP).

In Investigation Report 216-2018, 218-2018, the Commissioner found that an *application number* qualified as an "identifying number" and constituted personal information pursuant to the equivalent subsection 24(1)(d) of FOIP.

Subsection 23(1)(e)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;

An individual's home address, telephone, facsimile (fax number) or email address is personal information under LA FOIP.

LA FOIP should not be taken to say that names, addresses and telephone numbers of individuals in local authority records must never be disclosed. Rather, it requires that such information must not be disclosed if the protection of privacy of an individual so requires. Individuals engaged in discharging public functions obviously do not have the same expectation of privacy when so doing as when they are going about their personal or private affairs. If "personal information" is claimed as an exemption it should not be just any information about an individual, it must be personal in the sense that it is private and that it is or should be treated as confidential so that disclosure would amount to an invasion of privacy or a breach of confidence.[142]

To qualify as personal information, the information must be about the individual in a personal capacity. As a general rule, information associated with an individual in a professional, official, or business capacity will not be considered to be "about" the individual.[143]

The IPC has consistently found that "business card information" (contact information on a business card) does not constitute personal information because it is not personal in nature.[144]

Business telephone numbers and addresses would qualify as personal information only if the record was personal in nature.[145]

The Commissioner has previously relied on the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) to support the interpretation that contact information for individuals in commercial business or private industry is not personal information. PIPEDA applies to every organization that collects, uses, or discloses personal information during "commercial activities". Section 4.01 of PIPEDA, carves out business contact information from the type of personal information that requires protection. Subsection 2.1 of PIPEDA defines

---

[142] SK OIPC Review Report 1993-029 at p. 6. Also cited in Review Report F-2005-001 at [28].
[143] SK OIPC Review Report F-2010-001 at [126]. Originated from ON IPC Order PO-2420 at p. 3.
[144] SK OIPC Review Reports F-2006-001 at [113], F-2010-001 at [124], LA-2010-001 at [63], F-2012-006 at [138], LA-2013-002 at [84], F-2013-007 at [109], F-2014-001 at [352], F-2014-005 at [18], 158-2016 at [13], 184-2016 at [20], 207-2016 to 211-2016 at [28], 258-2016 at [13], 263-2016 to 268-2016 at [72], 277-2016 at [41] and [43], 290-2017 at [14], 302-2016 at [61], 071-2017, 072-2017, and 073-2017 at [57], 082-2017 at [20], 139-2017 at [94], 298-2017 at [19], 017-2018 at [49], 078-2018 at [48], 117-2018 at [22], 166-2018 at [114], 108-2019 at [146], 135-2019 at [57], 186-2019 at [30], 141-2019 at [20] and 147-2018, 197-2018, 008-2019, 073-2019 at [132].
[145] SK OIPC Review Report 302-2016 at [59].

"business contact information" as, "information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business, or profession" such as the individual's name, position name or title, work address, work telephone number, work fax number or work electronic address. This supports the conclusion that business card information is not meant to be personal information for the purposes of subsection 23(1)(e) of LA FOIP.[146]

Fingerprints are a mark made on a surface by a person's fingertip, especially as consisting of a unique pattern used for purposes of identification.[147]

IPC Findings

In Review Report F-2005-001, the Commissioner found that the *work phone numbers of government employees* were not personal information under the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP).

In Investigation Report F-2012-004, the Commissioner found that an *individual's home address* qualified as personal information pursuant to the equivalent provision in FOIP.

In Review Reports LA-2013-003 and 186-2019, the Commissioner found that a *personal email address* and an *internet protocol (IP) address* qualify as the "home address" of an individual and qualifies as personal information pursuant to subsection 23(1)(e) of LA FOIP.

In Review Report 277-2016, the Commissioner found that an employee's government assigned *cell phone number* and a *cell phone number for an owner of a private business* that was used for business purposes qualified as "business card information" and did not qualify as personal information pursuant to the equivalent provision in FOIP. In addition, the Commissioner found that the *names and contact information for lawyers* acting in their professional capacity was "business card information".

In Review Report 184-2016, the Commissioner found that the *work email address of an employee of the Global Transportation Hub* qualified as "business card information" and did not qualify as personal information pursuant to the equivalent provision in FOIP.

[146] See SK OIPC Review Reports F-2012-006 at [143] to [145], LA-2013-002 at [82] to [84], 186-2019 at [28] to [30].
[147] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 531.

In Review Report 207-2016 to 211-2016, the Commissioner found that the *telephone numbers of professional appraisers* acting in their capacity as professionals was "business card information" and not personal information.

In Review Report 082-2017, the Commissioner found that the contact information for an individual acting in their professional capacity (a *former employee's post office box number, town, province and postal code, telephone number, fax number and email address)* was "business card information" and was not personal information.

Subsection 23(1)(f)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(f) the personal opinions or views of the individual except where they are about another individual;

The personal views or opinions of an individual are that individual's personal information unless the views or opinions are about someone else.

Opinions are views or judgements not necessarily based on fact or knowledge.[148]

Views are particular ways of regarding something; an attitude or opinion.[149]

There is often confusion between subsections 23(1)(f), 23(1)(h) and 23(2)(b) of LA FOIP. All three provisions deal with views and opinions of individuals. The following examples will help clarify the three provisions:

23(1)(f) - the views or opinions expressed by an individual are the individual's personal information. For example, an individual writes, "I am a bad student" or "I think exercise is overrated". It is the individual's personal views or opinions about something and is therefore, the individual's personal information. If the views or opinions are about someone else – subsection 23(1)(h) of LA FOIP applies.

[148] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 999. See also SK OIPC Review Reports F-2006-004 at [43], LA-2013-003 at [26] and 139-2017 at [91].
[149] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 1598.

23(1)(h) - the views or opinions expressed by an individual about another individual are the personal information of the individual they are about. For example, an individual writes, "Smith is a bad student" or "Smith exercises but is still out of shape". The individual's opinion is about Smith so the opinion is Smith's personal information.

23(2)(b) – the views or opinions expressed by employees of a local authority, given in the course of employment, are not the personal information of the employee. For example, an employee writes, "I think we should proceed with this project" or "I think we are on the right course". An employee's views or opinions offered in terms of performing their jobs or offered in the course of preparing work product are not the employee's personal information. This is because the employee is only offering the opinion or view as part of their employment responsibilities, not in a personal capacity. However, if the employee states, "Smith is not a good employee", the opinion is about another individual and subsection 23(1)(h) of LA FOIP would apply.

Signing a petition is personal information pursuant to subsection 23(1)(f) of LA FOIP because by signing, the individual is indicating that they agree with the petition's purpose. This would constitute the opinions or views of the individual.[150] However, petitions are not intended to be kept secret. The names of individuals signing a petition are not normally supplied in confidence. Petitions are generally considered to be public information; individuals signing a petition are publicly lending their support to a position and expect that their names may be disclosed. There may be some cases, however, in which the circumstances surrounding the collection of signatures on a petition indicate that the individuals have signed with the understanding that their names will not be disclosed. Each situation must be considered on a case-by-case basis.[151]

IPC Findings

In Review Report F-2010-001, the Commissioner found that *opinions submitted by private individuals to a government institution* as part of a consultation process, was personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*. The Commissioner recommended the names and email addresses associated with the opinions be removed and the opinions be released as no individuals could then be identified.

[150] SK OIPC Review Report 156-2015 at [7]. This was also found in Investigation Report 059-2018 at [9].
[151] SK OIPC Investigation Report 059-2018 at [21] to [23].

In Review Report LA-2013-003, the Commissioner found that some employees provided views and opinions outside of the employee's duties and as such the carve-out at subsection 23(2)(b) of LA FOIP did not apply. For example, views or opinions that dealt with matters outside of the employee's duties were sent from a personal email address, contained personal contact information and the views or opinions did not represent the official views of the employer. These types of views or opinions were found to be personal information.

In Review Report 019-2014, the Commissioner found that information severed was not personal in nature and were the opinions and views of elected City of Saskatoon Councillors in the course of their official responsibilities and professional capacity. Other information severed were opinions and views of a contracted third party business related to a contract between the business and the City of Saskatoon. Again, the opinions and views were given in a professional capacity. The Commissioner recommended the information be released.

In Investigation Report 034-2015, the Commissioner found that a complainant's *conversations recorded on a city* bus qualified as the complainant's personal information because the conversations included the complainant's personal views and opinions.

In Review Report 277-2016, the Commissioner found that an *employee's personal opinions made about a sporting event* were the personal information of the employee's pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*. It was a conversation between colleagues regarding a shared personal interest and did not relate to government business.

In Review Report 258-2016, the Commissioner found that feedback employees provided to the employer that included *descriptions of personal feelings and concerns outside of professional and official capacities* was the personal information of the employees pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

In Review Report 071-2017, 072-2017, and 073-2017, the Commissioner found that the information in some letters was the personal information of the authors of the letters pursuant to subsection 23(1)(f) of LA FOIP. This included their work history and *descriptions of the impacts a workplace issue had upon them personally*.

In Review Report 139-2017, the Commissioner found that a witness statement contained mostly factual information about what a witness saw on the way to work the morning of a bomb threat. The Commissioner viewed the information as observation material and not opinions or views of a personal nature.

Subsection 23(1)(g)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(g) correspondence sent to a local authority by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;

Subsection 23(1)(g) of LA FOIP is intended to protect personal information that appears in correspondence sent to local authorities by individuals. In addition, it protects replies to the individuals' correspondence if those replies reveal the personal information in the original correspondence sent by the individual. The only exception is if the information is views or opinions about another individual which should then be considered under subsection 23(1)(h) of LA FOIP.

The following three questions can be asked to help determine if information is personal information pursuant to subsection 23(1)(g) of LA FOIP:

1. Is the information correspondence sent to a local authority by an individual?

Correspondence is letters sent or received.[152] In terms of this provision, the information must be correspondence "sent" to a local authority or the replies from the local authority.

Individual means natural persons (human beings).[153] Use of the word *individual* in this provision makes it clear that the protection provided relates only to a natural person or human being.[154]

---

[152] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 320, (Oxford University Press).
[153] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at pp. 924, 1238 and 1378.
[154] ON IPC Order 16 at p. 19. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 2, Scope of FIPPA – Who and What Falls under FIPPA* at p. 44. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_2.pdf. Accessed on April 24, 2020.

This provision requires that an 'individual' send the correspondence in question in a personal capacity, as opposed to in an official local authority or business capacity.[155]

About means on the subject of or concerning.[156] *About* an identifiable individual means the information is not just the subject of something but also relates to or concerns the subject.[157]

2. Is the information implicitly or explicitly of a private or confidential nature?

If the information is associated with the individual in their professional capacity, the information is not considered to be "about" the individual for purposes of this provision. The provision requires that an 'individual' send the correspondence in question in a personal capacity, as opposed to in an official local authority or business capacity.[158]

The terms "*implicitly*" and "*explicitly*" as they relate to confidentiality are found in other provisions of LA FOIP (sections 13, 18 and 30). The definitions below are consistent with Chapter 4, *Exemptions from the Right of Access*, sections 13, 18 and 30.

Implicitly means that the confidentiality is understood even though there is no actual statement of confidentiality, agreement, or other physical evidence of the understanding that the information will be kept confidential.[159]

Factors that can be considered include:

- What is the nature of the information
- Would a reasonable person regard it as confidential
- Would it ordinarily be kept confidential by a local authority or the individual that provided it[160]

---

[155] ON IPC Order MO-3332 at [18].
[156] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 4, (Oxford University Press).
[157] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII), [2007] 1 FCR 203. Also see the Office of the Privacy Commissioner of Canada resource, *PIPEDA Interpretation Bulletin: Personal Information*, 2013, available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/.
[158] ON IPC Orders PO-3180 at [44] and MO-3332 at [18].
[159] SK OIPC Review Reports F-2006-002 at [57], F-2009-001 at [62], F-2012-001/LA-2012-001 at [29], LA-2013-002 at [49], F-2014-002 at [47].
[160] Adapted from SK OIPC resource, *Guide to FOIP, Chapter 4, Exemptions from the Right of Access* at sections 13, 19 and 31. Originated from BC IPC Orders 331-1999 at [8], F13-01 at [23], PEI IPC Order FI-

Explicitly means that the request for confidentiality has been clearly expressed, distinctly stated, or made definite. There may be documentary evidence that shows that the information was obtained with the understanding that it would be kept confidential.[161]

Factors that can be considered include:

- Is there an express condition of confidentiality (i.e., something in writing that confirms it)?[162]
- Did the local authority or individual outline confidentiality intentions prior to the information being provided[163]

3. Is it a reply and would disclosure reveal the content of the original correspondence?

The provision also protects replies from the local authority to the individual if the replies reveal personal information from the original correspondence sent by the individual that is of a private or confidential nature.

For replies, disclosure must reveal the private or confidential personal information from the original correspondence. Local authorities should identify what information in the reply reveals the content of the original correspondence that is private or confidential. The exception is views or opinions that are caught by subsection 23(1)(h) of LA FOIP.

The provision explicitly excludes correspondence that contains views or opinions of the individual with respect to another individual. In these cases, see subsection 23(1)(h) of LA FOIP.

16-006 at [19] and Office of the Nova Scotia Information and Privacy Commissioner (NS IPC) Review Reports 17-03 at [34] and 16-09 at [44].

[161] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at pp. 104 and 105.

[162] Adapted from Adapted from SK OIPC resource, *Guide to FOIP, Chapter 4, Exemptions from the Right of Access* at sections 13, 19 and 31. See also SK OIPC Review Reports F-2006-002 at [56], LA-2013-003 at [113], F-2014-002 at [47]; PEI IPC Order 03-006 at p. 5; AB IPC Orders 97-013 at [23] to [24], 2001-008 at [54].

[163] Adapted from Adapted from SK OIPC resource, *Guide to FOIP, Chapter 4, Exemptions from the Right of Access* at sections 13, 19 and 31. See also SK OIPC Review Reports F-2006-002 at [56], F-2012-001/LA-2012-001 at [29], LA-2013-002 at [49], LA-2013-003 at [113], F-2014-002 at [47]; PEI IPC Order 03-006 at p. 5; AB IPC Order 97-013 at [25].

IPC Findings

In Investigation Report F-2012-004, the Commissioner found that a Saskatchewan Workers' Compensation Board (WCB) letter to a complainant contained details of another letter sent to the then Ministry of Advanced Education, Employment and Labour by an individual. The WCB letter appeared to be a reply to the original letter sent. Therefore, it constituted personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

In Investigation Report 275-2017, the Commissioner found that communications between SaskPower and the complainant that were shared with the Regina Police Service qualified as the personal information of the complainant pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

In Review Report 156-2017 & 264-2017, the Commissioner found that 11 pages withheld by the RM of Manitou Lake No. 442 (RM) did not contain personal information pursuant to subsection 23(1)(g) of LA FOIP. The 11 pages consisted of meeting notes and an unsolicited letter from the RM.

Subsection 23(1)(h)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(h) the views or opinions of another individual with respect to the individual;

The views or opinions someone has about another individual are the personal information of the individual they are about.

Opinions are views or judgements not necessarily based on fact or knowledge.[164]

Views are particular ways of regarding something; an attitude or opinion.[165]

[164] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 999. See also SK OIPC Review Reports F-2006-004 at [43], LA-2013-003 at [26] and 139-2017 at [91].
[165] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 1598.

There is often confusion between subsections 23(1)(f), 23(1)(h) and 23(2)(b) of LA FOIP. All three provisions deal with views and opinions of individuals. The following examples will help clarify the three provisions:

23(1)(f) - the views or opinions expressed by an individual are the individual's personal information. For example, an individual writes, "I am a bad student" or "I think exercise is overrated". It is the individual's personal views or opinions about something and is therefore the individual's personal information. If the views or opinions are about someone else – subsection 23(1)(h) of LA FOIP applies.

23(1)(h) - the views or opinions expressed by an individual about another individual are the personal information of the individual they are about. For example, an individual writes, "Smith is a bad student" or "Smith exercises but is still out of shape". The individual's opinion is about Smith so the opinion is Smith's personal information.

23(2)(b) – the views or opinions expressed by employees of a local authority, given in the course of employment, are not the personal information of the employee. For example, an employee writes, "I think we should proceed with this project" or "I think we are on the right course". An employee's views or opinions in terms of work product are not the employee's personal information. This is because the employee is only offering the opinion or view as part of their employment responsibilities, not in a personal capacity. However, if the employee states, "Smith is not a good employee", the opinion is about another individual and subsection 23(1)(h) of LA FOIP would apply.

IPC Findings

In Review Report F-2012-006, the Commissioner found that any *opinion offered about the applicant* constituted the applicant's personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

In Review Report LA-2013-001, the Commissioner found that *opinions of employees about the applicant* were the personal information of the applicant pursuant to subsection 23(1)(h) of LA FOIP. In addition, the Commissioner found that the *opinions expressed by employees about other persons* should be released to the applicant because the Commissioner was bound by *Liick v. Saskatchewan (Minister of Health)*, 1994 CanLII 4934 (SK KB) on similar facts. Were it not for the *Liick* decision, the Commissioner would have likely found the opinions expressed

by the employees about individuals other than the applicant was the personal information of those individuals pursuant to subsection 23(1)(h) of LA FOIP.

In Review Report LA-2014-002, the then Saskatoon Regional Health Authority (SRHA) severed portions of a letter that described the actions of two employees and why. The Commissioner found that the actions described were in the work context and did not constitute personal information. However, *the 'why' was an expressed personal opinion or view about an individual* and constituted the personal information that the opinion or view was about. Further, another portion severed was about an employee's performance and opinions or views about the employee. The Commissioner found the opinions or views of the employee were the employee's personal information.

In Review Report 239-2016, the Commissioner found that *opinions and views made about the applicant by fellow employees* was the personal information of the applicant.

In Review Report 071-2017, 072-2017, and 073-2017, the Commissioner found that staff members' opinions about the applicant were the personal information of the applicant pursuant to subsection 23(1)(h) of LA FOIP.

Subsection 23(1)(i)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;

The purpose of this provision is to identify as personal information that information which a local authority obtains from a taxpayer (on the taxpayer's return) or otherwise gathers relating to the taxpayer for the purpose of collecting a tax.[166]

[166] Similar interpretation taken by BC IPC and Office of the Newfoundland and Labrador Information and Privacy Commissioner (NFLD IPC). See BC IPC Order F05-29 at [92] and NFLD IPC Review Report A-2017-002 at [28].

Obtained means to acquire in any way; to get possession of; to procure; or to get a hold of by effort.[167]

As the Supreme Court of Canada has affirmed, "the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act and the intention" of the Legislature. As such, the word "*obtained*" does not cover information developed or created by a local authority.[168]

Tax return is a form used to report taxable income or property for federal, provincial, or municipal purposes and includes personal and property tax information.[169]

Gathered for the purpose of collecting a tax means the information was collected by authorities for the purpose of collecting due or overdue taxes, for a federal, provincial, or municipal government. For example, information gathered in a municipal tax return in relation to eligibility for a homeowner grant.[170]

Information needs to be collected for the sole or primary purpose of collecting a tax to qualify. Information collected for a different purpose but later used for collecting a tax would not qualify as having been "gathered for the purpose of collecting a tax".[171]

The word "*gathered*" does not cover information that was generated or created by a local authority by applying skills, techniques, and professional judgement to information that it has gathered (even where underlying information that is analyzed to create the disputed information has been gathered directly from a taxpayer).[172]

Local authorities may gather information relating to the taxpayer from a variety of sources – including sources other than tax returns and sources other than the taxpayer – and then record that information. Such information, in the state in which it was gathered or as

---

[167] Originated from Campbell Black, Henry, 1990. *Black's Law Dictionary, 6th Edition.* St. Paul, Minn.: West Group. Adopted by AB IPC in Order 2000-021 at [26]. Adopted in SK OIPC Review Report F-2006-001 at [58] and [59]. Also, found in SK OIPC Review Report F-2006-002 at [39].
[168] BC IPC Order F05-29 at [90] to [91].
[169] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[170] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[171] See BC IPC Orders 00-10 at p. 20 and F15-19 at [24].
[172] See BC IPC Orders F05-29 at [96] and F15-19 at [25].

compiled in the local authority's records or files, will be information that has been "gathered" for purposes of this provision.[173]

"*Gathered*" includes information relating to the taxpayer that is gathered by a local authority without the taxpayer's positive or consensual involvement, or even knowledge.[174]

Tax means provincial, municipal, or federal tax. It does not include licence fees, stumpage fees, royalties, municipal development costs charges levied on developments or other fees assessed in relation to a direct benefit received by the party paying the fee.[175]

On several occasions, the Office of the Information and Privacy Commissioner of British Columbia (BC IPC) has examined issues related to its similarly worded provision in its *Freedom of Information and Protection of Privacy Act* (FIPPA). In BC IPC Order F15-19, information pertaining to tax liabilities were ordered disclosed because the information involved aggregate information generated by the BC Ministry of Finance in relation to five properties, not information of individual property owners. Had individual records been sought, it is fair to conclude from the following that the information would have been deemed personal information gathered for the purpose of determining tax liability or collecting a tax.[176]

The Office of the Information and Privacy Commissioner of Newfoundland and Labrador found that the information contained on T4s for a town manager, clerk and head of maintenance was gathered for the purpose of determining tax liability[177] or collecting a tax.[178] As such, it was withheld from the applicant.

IPC Findings

In Review Report LA-2007-002, an applicant sought the complete tax roll for the Rural Municipality of Edenwold No. 158 (RM). Upon review, the Commissioner found that the record included information about a named individual that was obtained by the RM for the purpose of collecting a tax, namely the property tax enabled by *The Rural Municipality Act,*

[173] BC IPC Order F05-29 at [97].
[174] BC IPC Order F05-29 at [95].
[175] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[176] BC IPC Order F15-19 at [28]. See also NFLD IPC Review Report A-2017-002 at [27].
[177] The provision in the NFLD *Access to Information Protection of Privacy Act* includes "determining tax liability" in its equivalent provision. This is also the case with BC's provision.
[178] NFLD IPC Review Report A-2018-018 at [16].

1989. As such, the information was the personal information of the individual pursuant to subsection 23(1)(i) of LA FOIP.

In Investigation Report F-2012-004, the Commissioner found that taxation information qualified as personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*. This included taxation information such as province of employment and federal tax exemption.

Subsection 23(1)(j)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness;

Finances means the money resources of a person. For example, a how much an individual property owner is in arrears on their taxes or how much they hold in their bank account.[179]

Assets are items owned that have value. For example, the entries on a balance sheet showing the items of property owned, cash and vehicles.[180]

Liabilities are financial or pecuniary obligations in a specified amount; debt.[181]

Net worth means the total wealth held by a person; a measure of one's wealth, usually calculated as the excess of total assets over total liabilities.[182]

Bank balance means a figure representing the difference between credits and debits in an account; the amount of money held in an account.[183]

---

[179] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions#f. Accessed May 12, 2020.
[180] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 145.
[181] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1097.
[182] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1927.
[183] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 101.

Financial history or activities refer to any past information about an individual's monetary activities, whether that information has been collated or not. For example, a list of an individual's investments.[184]

Credit worthiness relates primarily to an individual's credit rating but includes any information by which the individual's financial standing can be ascertained or surmised. For example, an individual's credit rating.[185]

IPC Findings

In Investigation Report F-2012-002, the Commissioner found that a statement collected by the Saskatchewan Workers' Compensation Board revealed that the complainant had a farm, which was an asset. Therefore, the information in the statement qualified as personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

In Review Report F-2013-006, the Commissioner found that information pertaining to an individual's assets lost and the value of the assets qualified as the individual's assets. As such, it constituted the individual's personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

In Investigation Report 072-2014, the Commissioner found that, the balance owing on a complainant's Saskatchewan Telecommunications cell phone account qualified as the complainant's liabilities. As such, it constituted the complainant's personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

[184] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[185] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Subsection 23(1)(k)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(k) the name of the individual where:

(i) it appears with other personal information that relates to the individual; or

(ii) the disclosure of the name itself would reveal personal information about the individual.

A name alone is not personal information unless release of the name itself would reveal personal information about the individual.[186]

Subsection 23(1)(k) of LA FOIP deals with the names of individuals and when they constitute personal information. Subsection 23(1)(k) of LA FOIP provides two types of situations where the name of an individual could constitute personal information:

1. The name is personal information when it appears with other personal information.

For example, several protestors are arrested during a demonstration. The police service has a record titled, *Demonstrators Arrested*. It contains a list of names of demonstrators arrested. Even though the record only contains a list of names, by appearing on this list, it reveals that the individuals were arrested which is personal information (criminal history – subsection 23(1)(b) of LA FOIP). In such a context, the name appears with other personal information (i.e., the title of the record).

2. Disclosing the name alone would reveal personal information about the individual.

For example, several protestors are arrested during a demonstration. The police service has a record that lists the names of demonstrators arrested, but nothing more is revealed on this record. The media has reported that several demonstrators were arrested so the public is

[186] See subsection 24(1)(k)(ii) of FOIP. First cited in SK OIPC Review Report 2003-014 at [26]. Later referenced in SK OIPC Review Report F-2005-001 at [13]. See also SK OIPC Review Reports F-2012-006 at [147], F-2014-005 at [10], 195-2015 and 196-2015 at [17] and 112-2018 at [46]. See also *General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance*, 1993 CanLII 9128 (SK CA) at [14] and *Griffiths v. Nova Scotia (Education)*, 2007 NSSC 178 (CanLII) at [24].

aware. Even though the record only contains a list of names with no context in terms of what the names on the list pertain to, there is already information available publicly that could be linked to these names which could reveal the individuals were arrested. The fact that someone has been arrested qualifies as their personal information (criminal history – subsection 23(1)(b) of LA FOIP). In this context, the name alone on the record would reveal personal information (i.e., the name can be linked to already available information).

The names of employees of a local authority and their respective work telephone numbers are not personal information under LA FOIP.[187]

Subsection 23(1)(k)(i)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

…

(k) the name of the individual where:

(i) it appears with other personal information that relates to the individual;

A name alone is not personal information unless release of the name itself would reveal personal information about the individual.[188]

An individual's name may appear with other personal information in a record. The inclusion of a name in a record often makes the other personal information in the record about an "identifiable individual". Where possible, local authorities should consider severing the name and releasing the other information as removal of the name makes the other information de-identified, in most cases. Alternatively, release the name and sever the other personal information. This is consistent with section 8 of LA FOIP which provides:

[187] SK OIPC Review Reports F-2005-001 at [29], F-2008-001 at [87].
[188] See subsection 24(1)(k)(ii) of FOIP. First cited in SK OIPC Review Report 2003-014 at [26]. Later referenced in SK OIPC Review Report F-2005-001 at [13]. See also SK OIPC Review Reports F-2012-006 at [147], F-2014-005 at [10], 195-2015 and 196-2015 at [17] and 112-2018 at [46]. See also *General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance*, 1993 CanLII 9128 (SK CA) at [14] and *Griffiths v. Nova Scotia (Education)*, 2007 NSSC 178 (CanLII) at [24].

8 Where a record contains information to which an applicant is refused access, the head shall give access to as much of the record as can reasonably be severed without disclosing the information to which the applicant is refused access.

However, local authorities should be aware that in some cases, removal of an individual's name alone does not necessarily qualify personal information as sufficiently de-identified. The ability to re-identify is increased when information contains unique characteristics (e.g., unusual occupation, unusual death, or event) or where external sources of information can be used to identify individuals (e.g., voter registration records, newspapers, obituaries, social media sites, and other public registries).[189] For more on de-identification, see *De-identified information* later in this Chapter.

The names of employees of a local authority and their respective work telephone numbers are not personal information under LA FOIP.[190]

IPC Findings

In Review Report 2003-042, the Commissioner found that names severed from an internal memo by the Ministry of Social Services was appropriate because releasing the names would identify that the individuals were recipients of social assistance and thus disclose financial history of the individuals.

In Investigation Report F-2012-003, the Commissioner found that the equivalent provision in *The Freedom of Information and Protection of Privacy Act* applied to the names of four employees listed on a two-page audit report, because the names appeared with other personal information. The report contained the total number of hours worked, rate of pay per hour, total amount paid, total vacation paid and the total gross and net paid for each employee. The employer was not a government institution, so subsection 24(2)(a) of *The Freedom of Information and Protection of Privacy Act* did not to apply.

In Investigation Report LA-2013-002, the Commissioner found that photographs of individuals are personal in nature. Further, photographs of identifiable employees plus their names, qualified as personal information pursuant to subsection 23(1)(k)(i) of LA FOIP.

In Investigation Report F-2014-001, the Commissioner found that the information contained in a document titled, "Decision of the Appeals Department", qualified as the complainant's

[189] SK OIPC Review Report F-2014-005 at [22] to [23].
[190] SK OIPC Review Reports F-2005-001 at [29], F-2008-001 at [87].

personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*. The Complainant's name along with other information of a personal nature (diagnoses, tests, and treatments) were contained in the record.

In Review Report F-2014-001, the Commissioner found that an employee's name in a record qualified as personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP) because the name appeared along with a reference to the employee attending a personal family function. In addition, the Commissioner found the name of an individual who was a member of the public was personal information pursuant to subsection 24(1)(k)(i) of FOIP because the name appeared along with a personal home email address.

Subsection 23(1)(k)(ii)

Interpretation

23(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:

...

(k) the name of the individual where:

...

(ii) the disclosure of the name itself would reveal personal information about the individual.

A name alone is not personal information unless release of the name itself would reveal personal information about the individual.[191]

A list of names of unsuccessful applicants for a job competition constitutes personal information pursuant to subsection 23(1)(k)(ii) of LA FOIP. Disclosure of the names would reveal the fact that certain individuals applied for a job and were unsuccessful.[192]

---

[191] See subsection 24(1)(k)(ii) of FOIP. First cited in SK OIPC Review Report 2003-014 at [26]. Later referenced in SK OIPC Review Report F-2005-001 at [13]. See also SK OIPC Review Reports F-2012-006 at [147], F-2014-005 at [10], 195-2015 and 196-2015 at [17] and 112-2018 at [46]. See also *General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance*, 1993 CanLII 9128 (SK CA) at [14] and *Griffiths v. Nova Scotia (Education)*, 2007 NSSC 178 (CanLII) at [24].

[192] SK OIPC Review Report 112-2018 at [47]. See also ON IPC Order MO-3355 at [11].

When considering if a name alone reveals personal information about an individual, local authorities should consider the type of document the name appears in and what type of information is already in the public domain. For example, media stories, obituaries, and social media sites.

IPC Findings

In Review Report F-2013-007, the Commissioner found that if the name alone were released in that case it would be possible for the applicant to link the name with other details about the individual of a personal nature that had previously been released to the applicant. The applicant could piece the information together resulting in an identifiable individual.

In Review Report F-2014-005, the Commissioner found that the name of victims in the records constituted personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*. Release of the names alone would reveal the fact that the individuals were the victim of a teacher's professional misconduct or incompetence due to the nature of the records and the information already released to the applicant.

Subsection 23(1.1)

Interpretation

23(1.1) On and after the coming into force of subsections 4(3) and (6) of *The Health Information Protection Act*, with respect to a local authority that is a trustee as defined in that Act, **"personal information"** does not include information that constitutes personal health information as defined in that Act.

If a local authority is also a trustee under *The Health Information Protection Act* (HIPA), LA FOIP would not apply to information that qualifies as personal health information under HIPA. The local authority should apply HIPA to that personal health information instead of LA FOIP.

The purpose of this provision is to ensure that two different laws do not apply to the same information at the same time.[193]

[193] SK OIPC Investigation Report F-2010-001 at [31].

To clarify further, all government institutions under *The Freedom of Information and Protection of Privacy Act* also qualify as trustees under HIPA (see s. 2(t)(i) of HIPA). However, not all local authorities qualify as trustees under HIPA.

Two provisions in LA FOIP cover off "personal health information" held by local authorities. Subsections 23(1)(c) and 23(1.1) of LA FOIP:

> **23(1)(c) of LA FOIP**: The purpose of this provision is to ensure privacy protection for personal health information in the possession or control of a local authority where the local authority is **not** also a trustee under *The Health Information Protection Act* (HIPA).
>
> **23(1.1) of LA FOIP:** The purpose of this provision is to ensure privacy protection for personal health information in the possession/custody or control of a local authority that **is also** a trustee under HIPA.

An example of a local authority that also qualifies as a trustee under HIPA is the Saskatchewan Health Authority. It is both a local authority under subsection 2(f)(xiii) of LA FOIP and also a trustee pursuant to subsection 2(t)(ii) of HIPA. For personal health information in the custody or control of local authorities that are also trustees, HIPA applies to that personal health information and not LA FOIP (as per s. 4(3) of HIPA which states LA FOIP does not apply to personal health information). Subsection 4(3) of HIPA provides as follows:

> **4**(3) Except where otherwise provided, *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act* do not apply to personal health information in the custody or control of a trustee.

However, for local authorities that are not also trustees, LA FOIP would apply to certain personal health information described in LA FOIP (like subsection 23(1)(c) of LA FOIP). For example, the Regina Police Service is a local authority under subsection 2(f)(viii.1) of LA FOIP but is not a trustee under subsection 2(t) of HIPA. Therefore, provisions like subsection 23(1)(c) of LA FOIP would be engaged to protect personal health information collected, used or disclosed by the RPS in the carrying out of its work. That personal health information is treated as "personal information" under LA FOIP.

It is important to clarify, that where an organization qualifies as both a local authority and a trustee, LA FOIP does not apply to personal health information in the possession or control of

the local authority. Rather, HIPA applies to that information. Subsection 2(m) of HIPA defines **personal health information** as:

> **2**(m) **"personal health information"** means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or
> (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;[194]

To summarize how to approach personal health information in the possession or control of a local authority:

- If the local authority is also a trustee, HIPA should be relied on for the protection of personal health information.
- If the local authority is not also a trustee, LA FOIP should be relied on (only as provided for in LA FOIP) for the protection of personal health information.

IPC Findings

In Investigation Report 113-2020, the Commissioner investigated an alleged breach of privacy involving the Saskatchewan Health Authority (SHA). The complaint alleged the SHA used and disclosed the complainant's personal health information during a grievance process

[194] *The Health Information Protection Act*, SS 1999, c H-0.021 at subsection 2(m).

without authority. During the investigation, the Commissioner had to determine if LA FOIP or *The Health Information Protection Act* (HIPA) was engaged. As the SHA was both a local authority and a trustee and the information at issue was personal health information, the Commissioner determined that HIPA was engaged in the matter. This determination was based on subsection 23(1.1) of LA FOIP and subsection 4(3) of HIPA.

In Investigation Report 045-2021 et al., the Commissioner investigated numerous misdirected faxes that went astray. In one instance, a misdirected fax originated from the Department of Pediatrics at the College of Medicine at the University of Saskatchewan (U of S). The Commissioner determined that the U of S was not a trustee under *The Health Information Protection Act* (HIPA). However, it was a local authority as defined under subsection 2(f)(xi) of LA FOIP. Therefore, the Commissioner determined that subsection 23(1.1) of LA FOIP did not apply for the information involving the U of S. As the U of S was only a local authority, and not a trustee under HIPA, the information in the misdirected fax qualified as "personal information" pursuant to subsection 23(1)(c) of LA FOIP. Further, that LA FOIP was engaged on the matters involving the misdirected fax from the U of S.

Subsection 23(2)(a)

Interpretation

23(2) **"Personal information"** does not include information that discloses:

(a) the classification, salary, discretionary benefits or employment responsibilities of an individual who is or was an officer or employee of a local authority;

The purpose of subsection 23(2)(a) of LA FOIP is to allow the release of information about employment benefits and responsibilities of public servants, allowing a degree of transparency in relation to the compensation and benefits provided.[195]

[195] Adapted from AB IPC Orders 98-014 at [12] and F2003-002 at [23]. Alberta's subsection 17(2)(e) *Freedom of Information and Protection of Privacy Act* RSA 2000, c-F-25, is somewhat similar to Saskatchewan's subsection 23(2)(a) of LA FOIP. One difference is that is considers what is an unreasonable invasion of a person's privacy. In Alberta's Act, disclosing the classification, salary range, discretionary benefits or employment responsibilities as an officer, employee, or member of a public body or as a member of the staff of a member of the Executive Council is considered to not be an unreasonable invasion of privacy.

The definition of personal information does not include certain employment related information about officers or employees of a local authority. When information does not constitute personal information, the rules under Part IV of LA FOIP do not apply.

Classification means a category into which something is put.[196]

Salary means an agreed upon compensation for services usually paid at regular intervals on a yearly basis as distinguished from an hourly basis.[197] A fixed regular payment made by an employer to an employee.[198]

Discretionary benefits:

Discretionary means a choice given to a decision-maker as to whether, or how, to exercise a power.[199] Involves the exercise of judgement and choice.[200]

Benefit means an advantage or profit gained from something.[201] Benefit connotes some advantage or betterment.[202] A favourable or helpful factor or circumstance.[203]

In order for a benefit to be discretionary, the decision-maker must have a choice as to whether, or how, to grant the benefit. There must not be a duty to grant the "benefit".[204]

Employment responsibilities encompasses those duties that an individual is charged with performing as an officer or employee of the local authority.[205] A job title or position is information about employment responsibilities.[206]

Employee is defined at subsection 2(b.1) of LA FOIP as "an individual employed by a local authority and includes an individual retained under a contract to perform services for the local authority".

---

[196] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 263, (Oxford University Press).
[197] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1603.
[198] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 22.
[199] AB IPC Order 98-014 at [16].
[200] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 586.
[201] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 126, (Oxford University Press).
[202] *Hans v. STU*, 2016 NBKB 49 (CanLII) at [29].
[203] SK OIPC Review Reports LA-2009-001 at [90] to [92] and 082-2017 at [18].
[204] AB IPC Order 98-014 at [16].
[205] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 22.
[206] AB IPC Orders 2001-020 at [24] and F2003-002 at [25].

Severance payments arise in contemplation of the termination of employment. They arise in one of three ways: contractual provision, negotiated settlement or court ordered. Regardless of their origin, all three types are intended to address the issue of termination of employment without cause. Severance payments are either actual (court ordered) or estimated (contractual provision) damages for breach of contract. They are characterized and calculated as "pay in lieu of notice" but their essential character is that of damages. Their purpose is to place the terminated party in the position he or she would have been in but for the breach of contract. Severance payments cannot be considered as bestowing any advantage or betterment on the recipient. Unlike a bonus or employer pension contribution, there is no advantage bestowed. The term "benefit" cannot be interpreted to include severance payments. Therefore, severance payments qualify as personal information and do not fit under the definition of "discretionary benefits" pursuant to subsection 23(2)(a) of LA FOIP.[207]

IPC Findings

In Investigation Report 266-2017, the Commissioner found that information about an employee's duties did not qualify as the employee's personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*. Further, the hours that the employee worked was also found to not be the employee's personal information. In coming to this finding, the Commissioner considered *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC), [1997] 2 SCR 403 whereby the Supreme Court of Canada decided sign-in logs containing the name, dates and times individuals went to their workplaces constitute information about the position and was not personal information.

In Review Report 173-2018, the Commissioner found that severance payments did not qualify as a discretionary benefit. In coming to this finding, the Commissioner considered several court decisions including *Hans v. STU*, 2016 NBKB 49 (CanLII). Severance payments arise in contemplation of the termination of employment. They are characterized as "pay in lieu of notice" and their essential character is that of damages. The Commissioner still recommended Meewasin Valley Authority consider disclosure of the severance payment pursuant to subsection 29(2)(o) of *The Freedom of Information and Protection of Privacy Act* (public interest override equivalent to subsection 28(2)(n) of LA FOIP).

[207] *Hans v. STU*, 2016 NBKB 49 (CanLII) at [27] and 29]. See also SK OIPC Review Report 173-2018 at [12]. Further, see subsection 16(g)(ii) of *The Freedom of Information and Protection of Privacy Regulations*, RRS c F-22.01 Reg 1.

Subsection 23(2)(b)

Interpretation

23(2) **"Personal information"** does not include information that discloses:

…

(b) the personal opinions or views of an individual employed by a local authority given in the course of employment, other than personal opinions or views with respect to another individual;

Opinions are views or judgements not necessarily based on fact or knowledge.[208]

Views are particular ways of regarding something; an attitude or opinion.[209]

For an organization, public or private, to give voice to its views on a subject matter of interest to it, individuals must be given responsibility for speaking on its behalf. Views and opinions, which individuals express within the context of their employment responsibilities, are not personal opinions or views. Nor is the information "about" the individual. The individuals expressing the position of an organization, in the context or a public or private organization, act simply as a conduit between the intended recipient of the communication and the organization which they represent. The voice is that of the organization, expressed through its spokesperson, rather than that of the individual delivering the message.[210]

There is often confusion between subsections 23(1)(f), 23(1)(h) and 23(2)(b) of LA FOIP. All three provisions deal with views and opinions of individuals. The following examples will help clarify the three provisions:

23(1)(f) - the views or opinions expressed by an individual are the individual's personal information. For example, an individual writes, "I am a bad student" or "I think exercise is overrated". It is the individual's personal views or opinions about something and is therefore the individual's personal information. If the views or opinions are about someone else – subsection 23(1)(h) of LA FOIP applies.

23(1)(h) - the views or opinions expressed by an individual about another individual are the personal information of the individual they are about. For example, an individual

---

[208] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 999. See also SK OIPC Review Reports F-2006-004 at [43], LA-2013-003 at [26] and 139-2017 at [91].
[209] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 1598.
[210] ON IPC Reconsideration Order R-980015 at p. 17.

writes, "Smith is a bad student" or "Smith exercises but is still out of shape". The individual's opinion is about Smith so the opinion is Smith's personal information.

24(2)(b) – the views or opinions expressed by employees of a local authority, given in the course of employment, are not the personal information of the employee. For example, an employee writes, "I think we should proceed with this project" or "I think we are on the right course". An employee's views or opinions in terms of work product are not the employee's personal information. This is because the employee is only offering the opinion or view as part of their employment responsibilities, not in a personal capacity. However, if the employee states "Smith is not a good employee", the opinion is about another individual and subsection 23(1)(h) of LA FOIP would apply.

IPC Findings

In Review Report F-2006-001, the Commissioner found that information in a record showing the *opinion or comments of a fire fighter who completed a report* about a particular file intended to be furnished to the Office of the Fire Commissioner would be "work product" information and therefore not personal information of the public sector employee.

In Review Report LA-2013-001, the Commissioner found that the *views, opinions and comments made by employees who were witnesses in a harassment investigation* were not the personal information of the employees pursuant to subsection 23(2)(b) of LA FOIP. The witnesses in question were all employees of the then Regina Qu'Appelle Regional Health Authority (RQRHA) and their statements related to things they did or said in the course of their employment. Further, the Commissioner found that opinions or views the employees of RQRHA gave in the course of their employment that related to or were about the applicant was the personal information of the applicant and must be released to the applicant.

In Review Report LA-2013-003, the Commissioner found that an email written by an employee of the then Saskatoon Regional Health Authority *describing the functions of the area the employee worked and the impact of a location change on the functions in the employee's work area* was not the personal information of the employee. The views or opinions were provided in the employee's professional capacity. In addition, the contents of a Consensus Statement appeared to be the *collective opinion or view of a department given in the course of employment by several employees* and did not constitute personal information. In other words, the employees who signed the Consensus Statement appeared to be speaking on behalf of its department, not on behalf of themselves personally. However, some employees provided *views and opinions that were outside of the employee's duties*. For

example, views or opinions that dealt with matters outside of the employee's duties, were sent from a personal email address, contained personal contact information and the views or opinions did not represent the official views of the employer. These types of views or opinions were found to be personal information.

In Review Report LA-2014-002, the then Saskatoon Regional Health Authority severed portions of a letter that described the actions of two employees and why. The Commissioner found that the *actions described were in the work context* and did not constitute personal information. However, *the 'why' was an expressed personal opinion or view about an individual* and constituted the personal information that the opinion or view was about.

In Review Report 019-2014, the Commissioner found that information severed was not personal in nature and were the opinions and views of elected City of Saskatoon Councillors in the course of their official responsibilities and professional capacity. Other information severed were opinions and views of a contracted third party businesses related to a contract between the business and the City of Saskatoon. Again, the opinions and views were given in a professional capacity. The Commissioner recommended the information be released.

Subsection 23(2)(c)

Interpretation

23(2) **"Personal information"** does not include information that discloses:

…

(c) financial or other details of a contract for personal services;

The rationale for subsection 23(2)(c) of LA FOIP is that the public is entitled to know from whom and for what amount such services were purchased. This is an important part of public accountability.[211]

[211] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 24.

Financial means of or pertaining to revenue or money matters.[212] **Financial details** relates to the amounts paid under the contract.[213] Other examples include the hourly rate, monthly and total hours, total contract cost and the manner of calculating it.[214]

Details mean a number of particulars; an aggregate of small items.[215]

Other details include the names of the parties, the subject of the contract and standard boilerplate terms and conditions. Other details would not include résumés of employees of contractors that may be attached as an appendix to the contract.[216]

Contract means an agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law.[217]

Personal services mean beneficial or useful acts performed on behalf of another by an individual personally. In this sense, a personal service is an economic service involving either the intellectual or the manual personal effort of an individual, as opposed to the saleable product of the person's skill.[218]

Services means the performance of some useful act or series of acts for the benefit of another, usually for a fee; an intangible commodity in the form of human effort, such as labour, skill, or advice.[219]

Personal services contract (also termed a *performance contract*) means a contract that requires a party to act personally and does not allow substitution. People who provide

---

[212] *The Shorter Oxford English Dictionary on Historical Principles*, Oxford University Press 1973, Volume 1 at p. 964.
[213] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 24. Similar definition in Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 5, Exceptions to Disclosure* at p. 71. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_5.pdf. Accessed on June 5, 2020.
[214] AB IPC Order F2004-014 at [36].
[215] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[216] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 24.
[217] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 402.
[218] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1381.
[219] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1643.

unique personal services often make performance contracts. A contract that allows the contractor to choose the means to achieve the end result.[220]

It is important to determine if the relationship at issue is one of "employer-employee" on the one hand, or one of "fee-for-service" or "independent contractor" on the other. The Supreme Court of Canada has recently clarified the language - "contract of service" (employee) and "contract for services" (independent contractor) - to distinguish the two concepts.[221] Subsection 23(2)(c) of LA FOIP covers only "contract for services" or "fee-for-service" relationships as employment relationships are already covered under subsection 23(2)(a) of LA FOIP and would result in redundancy in the Act.[222]

Subsection 23(2)(c) of LA FOIP supports the policy goal of transparency for expenditures of public funds for employment and the purchase of services.[223]

IPC Findings

As of the date of this Chapter, no reports have been issued on this provision.

Subsection 23(2)(d)

Interpretation

23(2) **"Personal information"** does not include information that discloses:

> ...
>
> (d) details of a licence, permit or other similar discretionary benefit granted to an individual by a government institution;

Details means a number of particulars; an aggregate of small items.[224]

---

[220] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 408 and 409.
[221] AB IPC Order F2004-014 at [26]. See also ON IPOC Orders M-373, M-498 and *671122 Ontario Ltd. v. Sagaz Industries Canada Inc.*, 2001 SCC 59 (CanLII), [2001] 2 SCR 983 at [41].
[222] See AB IPC Order F2004-014 at [32].
[223] AB IPC Order F2004-014 at [38].
[224] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Details of a licence: In *Shook Legal, Ltd v Saskatchewan (Government Insurance)*, 2018 SKKB 238 (CanLII), the court found that "*details of a licence*" included the name, address and description of the vehicle being licensed, which included the vehicle identification number (VIN). Further, a licence plate is not afforded any level of privacy or protection and is equally available to one who observes any vehicle.

"*Details of a licence or permit*" does not contemplate release of a core of personal data that one provides in confidence. One must take a practical approach when confronted with an issue of interpretation of LA FOIP. It has endeavored to provide a workable balance between the interests of public access and protection of legitimate personal privacy issues. In passing upon this question, one must examine the effect that disclosure would have on the interest that the exemption in subsection 23(1) of LA FOIP seeks to protect. In some instances, licence applications might contain significant personal details.[225]

Licence or **permit** means written authorization from a local authority to carry out a named activity. For example, a licence may grant permission to own a dog or gun or carry on some trade.[226]

Other similar discretionary benefit refers to any details of an allowance similar to a license or permit given by a local authority. The nature of these other benefits must be discretionary, that is, the local authority must have a choice as to whether to provide this allowance.[227]

The words "other similar discretionary benefit" implies that "licence" and "permit" must also have the characteristics of being a "discretionary benefit".[228]

Some examples that could be captured under subsection 23(2)(d) of LA FOIP include:

- The names of licensed dog owners
- The details of a building permit (permit number, applicant's name, property address, construction authorized, application fee and expiry date)

---

[225] *General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance*, 1993 CanLII 9128 (SK CA) at [14] and [16]. Also quoted in *Shook Legal, Ltd v Saskatchewan (Government Insurance)*, 2018 SKKB 238 (CanLII) at [22] and [23].
[226] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[227] British Columbia Government Services, *FOIPPA Policy and Procedures Manual* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/disclosure-harmful-personal-privacy. Accessed April 29, 2020.
[228] AB IPC Order 98-018 at [18].

- The names of individuals to whom hunting licenses have been issued[229]

Discretionary benefits:

Discretionary means a choice given to a decision-maker as to whether, or how, to exercise a power.[230] Involves the exercise of judgement and choice.[231]

Benefit means an advantage or profit gained from something.[232] Benefit connotes some advantage or betterment.[233] A favourable or helpful factor or circumstance.[234]

For a benefit to be discretionary, the decision-maker must have a choice as to whether, or how, to grant the benefit. There must not be a duty to grant the "benefit".[235]

This provision does not apply to background personal information required by the local authority or provided voluntarily by an individual applying for the licence, permit or other similar discretionary benefit. This is supported by subsection 23(3) of LA FOIP which states this type of background information provided by an individual is personal information:

23(3) Notwithstanding clauses 2(d) and (e), **"personal information"** includes information that:

(a) is supplied by an individual to support an application for a discretionary benefit; and
(b) is personal information within the meaning of subsection (1).

[229] British Columbia Government Services, *FOIPPA Policy and Procedures Manual* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/disclosure-harmful-personal-privacy. Accessed April 29, 2020.
[230] AB IPC Order 98-014 at [16].
[231] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 586.
[232] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 126, (Oxford University Press).
[233] *Hans v. STU*, 2016 NBKB 49 (CanLII) at [29].
[234] SK OIPC Review Reports LA-2009-001 at [90] to [92] and 082-2017 at [18].
[235] AB IPC Order 98-014 at [16].

IPC Findings

In Investigation Report LA-2005-003, the Commissioner found that the details of a building permit would not be considered personal information pursuant to subsection 23(2)(d) of LA FOIP.

In Review Report F-2005-007, the Commissioner found that the name of a registered vehicle owner plus information about past damage to the vehicle would not be personal information of the individual.

In Review Report F-2013-003, the Commissioner found that a driver's name and address in Saskatchewan Government Insurance's database would be considered driver's licence information and therefore not personal information pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

In Review Report 116-2016, the Commissioner found the names of individuals who had leased protected lands would not be personal information as the leasing of protected lands qualified as a discretionary benefit pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act*.

Subsection 23(2)(e)

Interpretation

23(2) **"Personal information"** does not include information that discloses:

...

(e) details of a discretionary benefit of a financial nature granted to an individual by a local authority;

Subsection 23(2)(e) of LA FOIP provides that details of a discretionary benefit of a financial nature granted to an individual by a local authority is not personal information.

Details means a number of particulars; an aggregate of small items.[236] *Details of a financial discretionary benefit* are not limited to the amount paid to the third party, but include the

[236] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

third party's name, the reasons for providing the benefit and any consideration given to the local authority in exchange for granting the benefit.[237]

Discretionary benefits:

Discretionary means a choice given to a decision-maker as to whether, or how, to exercise a power.[238] Involves the exercise of judgement and choice.[239]

Benefit means an advantage or profit gained from something.[240] Benefit connotes some advantage or betterment.[241] A favourable or helpful factor or circumstance.[242]

For a benefit to be discretionary, the decision-maker must have a choice as to whether, or how, to grant the benefit. There must not be a duty to grant the "benefit".[243]

Discretionary benefit of a financial nature is any monetary allowance provided at the choice of the local authority.[244] Some examples include:

- Grants – "grant" means to give or confer discretionary benefits in situations where there is no requirement by the grantor to provide such benefits. The fact an individual received a grant, and the amount and purposes of the grant would be "details of a discretionary benefit" for purposes of subsection 23(2)(e) of LA FOIP.
- Scholarships[245]
- Donations[246]

---

[237] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 25. See also Government of Newfoundland and Labrador ATIPP Office, *Access to Information Policy and Procedures Manual*, October 2017 at p. 98.
[238] AB IPC Order 98-014 at [16].
[239] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 586.
[240] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 126, (Oxford University Press).
[241] *Hans v. STU*, 2016 NBKB 49 (CanLII) at [29].
[242] SK OIPC Review Reports LA-2009-001 at [90] to [92] and 082-2017 at [18].
[243] AB IPC Order 98-014 at [16].
[244] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020. See also Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 25.
[245] SK OIPC Review report 158-2018 at [76]. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 5, Exceptions to Disclosure* at p. 72. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_5.pdf. Accessed on June 5, 2020, and Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 25.
[246] NFLD IPC Report A-2008-011 at [68]. See also SK OIPC Review Report LA-2009-001 at [90].

This provision does not apply to background personal information required by the local authority or provided voluntarily by an individual applying for the benefit.[247] This is supported by subsection 23(3)(a) and (b) of LA FOIP which states that this type of information is still personal information in spite of subsections 23(2)(d) and (e) of LA FOIP:

Interpretation

23(3) Notwithstanding clauses 2(d) and (e), **"personal information"** includes information that:

(a) is supplied by an individual to support an application for a discretionary benefit; and

(b) is personal information within the meaning of subsection (1).

IPC Findings

In Review Report 082-2017, the Commissioner found that the compensation amounts paid to a former contracted employee (independent contractor) found on an invoice was not personal information pursuant to subsection 23(2)(e) of LA FOIP. The subtotal, GST amount and balance due were also found to not qualify as personal information pursuant to subsection 23(2)(e) of LA FOIP.

In Review Report 158-2018, the Commissioner found that scholarship amounts constituted *details of a discretionary benefit of a financial nature* paid to students by the University of Regina. As such, the scholarship amounts were not personal information pursuant to subsection 23(2)(e) of LA FOIP.

[247] SK OIPC Review Report LA-2008-001 at [92] to [93]. See also Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 26.

Subsection 23(2)(f)

Interpretation

23(2) **"Personal information"** does not include information that discloses:

...

(f) expenses incurred by an individual travelling at the expense of a local authority;

Expenses means costs incurred in the performance of a job or task.[248] In this case, the job or task is travelling.

An example is travel reimbursement for local authority employees (including contracted employees) and any individual.[249]

Expenses can include costs of flights, gas, meals, hotels, kilometer reimbursements for use of personal vehicles and parking fees. Other expenses may also be incurred.

IPC Findings

In Review Report 082-2017, the Commissioner found that travel reimbursement amounts found on an invoice of a former contracted employee was an expense incurred by the individual travelling at the expense of a local authority and was not personal information pursuant to subsection 23(2)(f) of LA FOIP. In addition, a page from a calendar indicated that one of the students used a personal vehicle while working for the local authority and the distance travelled. This was also found to not be personal information pursuant to subsection 23(2)(f) of LA FOIP.

Subsection 23(3)

Interpretation

23(3) Notwithstanding clauses 2(d) and (e), **"personal information"** includes information that:

(a) is supplied by an individual to support an application for a discretionary benefit; and

[248] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 501.
[249] SK OIPC Review Report 082-2017 at [40].

(b) is personal information within the meaning of subsection (1).

To apply, both (a) and (b) must apply to the circumstances. This is evidenced by the use of "and" between the provisions.

The following two-part test can be applied:

1. Is the information "personal information" within the meaning of subsection 23(1)?

To qualify, the information must first be personal information.[250]

Personal information is only that of an identifiable individual. Companies do not qualify as an "identifiable individual".[251]

See *Section 23: Definition of Personal Information*, earlier in this Chapter for assistance with this question.

2. Did the individual supply the personal information to support an application for a discretionary benefit?

Supplied means provided or furnished.[252]

Personal information may qualify as "supplied" if it was directly supplied to a local authority by the individual, or where its disclosure would reveal or permit the drawing of accurate inferences with respect to the personal information supplied by the individual.[253]

Personal information can still be "supplied" even when the record originated with the local authority (i.e., records may contain or repeat personal information extracted from documents supplied by the individual).[254]

---

[250] SK OIPC Review Report 130-2015 at [25].
[251] SK OIPC Review Report 130-2015 at [25].
[252] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions#supplied. Accessed August 21, 2019.
[253] Adapted from criteria utilized for subsection 19(1)(b) of FOIP. See SK OIPC Review Reports F-2005-003 at [17], F-2006-002 at [40].
[254] Adapted from *Merck Frosst Canada Ltd. v. Canada (Health)*, [2012] 1 SCR 23, 2012 SCC 3 (CanLII) at [157].

Application means a formal request to an authority.[255]

Discretionary benefits:

Discretionary means a choice given to a decision-maker as to whether, or how, to exercise a power.[256] Involves the exercise of judgement and choice.[257]

Benefit means an advantage or profit gained from something.[258] Benefit connotes some advantage or betterment.[259] A favourable or helpful factor or circumstance.[260]

For a benefit to be discretionary, the decision-maker must have a choice as to whether, or how, to grant the benefit. There must not be a duty to grant the "benefit".[261]

IPC Findings

In Review Report 130-2015, the Commissioner considered the Ministry of Environment's application of the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP) to a list of the names of eight companies and two individuals that submitted mineral exploration proposals to the Ministry of Environment. The Ministry of Environment asserted the proposals qualified as applications for discretionary benefits described in subsection 24(3)(a) of FOIP. The Commissioner found that in order for subsection 24(3) of FOIP to apply, the criteria at both subsections (a) and (b) must apply. The Commissioner found that companies do not qualify as identifiable individuals so would not qualify as personal information as required by subsection 24(3)(b) of FOIP. Further, the Commissioner found that the mineral exploration proposals constituted work product and not personal information. Subsection 24(3) of FOIP was found to not apply.

---

[255] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 64, (Oxford University Press).
[256] AB IPC Order 98-014 at [16].
[257] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 586.
[258] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 126, (Oxford University Press).
[259] *Hans v. STU*, 2016 NBKB 49 (CanLII) at [29].
[260] SK OIPC Review Reports LA-2009-001 at [90] to [92] and 082-2017 at [18].
[261] AB IPC Order 98-014 at [16].

Section 23.1: Duty of local authority to protect

Duty of local authority to protect

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

(a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the personal information in its possession or under its control;

(ii) loss of the personal information in its possession or under its control; or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

Privacy breaches happen when personal information is collected, used, or disclosed in ways that do not follow the rules set out in LA FOIP. The media frequently report stories of lost and stolen laptops, hacked and lost databases, identity theft, various kinds of internet fraud and the general misuse of personal information. Most often, these stories involve personal information collected by the private sector.[262] However, sometimes, it is personal information collected by local authorities.

Section 23.1 of LA FOIP establishes a local authority's duty to protect personal information. This includes establishing policies and procedures to maintain administrative, technical, and physical safeguards that:

- Protect the integrity, accuracy, and confidentiality of personal information (23.1(a))
- Protect against any reasonably anticipated threat or hazard to the security or integrity of personal information (23.1(b)(i))
- Protect against loss of personal information (23.1(b)(ii))
- Protect against unauthorized access to or use, disclosure, or modification of personal information (23.1(b)(iii))

[262] AB IPC resource, *Personal Information Protection Act (PIPA), PIPA Advisory #8: Implementing Reasonable Safeguards* at p. 1.

- Ensure compliance with LA FOIP by its employees (23.1(c))[263]

A **policy** is a standard course of action that has been officially established by government, including local authorities.[264]

A **procedure** is an established or official way of doing something; a series of actions conducted in a certain order or manner.[265]

Local authorities should have **written** policies and procedures in place to guide employees with what is required by law concerning privacy protection for personal information. Without written policies and procedures, a local authority has not taken reasonable steps to safeguard personal information in its possession or control.[266]

The written policies and procedures should be:

- Relevant and up to date
- Deal with security, records management, and information management
- Make administrative roles and responsibilities well-defined and easy to follow[267]

Safeguards

Administrative, technical, and physical safeguards generally include administrative procedures, physical standards and technical security services and mechanisms.[268]

---

[263] Section 23.1 of LA FOIP was added to LA FOIP following the amendments that were proclaimed in January 2018. However, *The Health Information Protection Act* (HIPA) has had a similarly worded provision since it first came into force in 2003 (section 16). Much of the guidance in this section of the Guide comes from over 15 years of work by the SK OIPC on establishing guidance on HIPA's section 16.
[264] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1401.
[265] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 1139.
[266] SK OIPC Investigation Reports H-2011-001 at [114], F-2007-001 at [48] and LA-2013-003 at [54] to 57].
[267] Government of Newfoundland and Labrador, ATIPP Office, Department of Justice and Public Safety, *Protection of Privacy Policy and Procedures Manual,* June 2015, at p. 72.
[268] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 134. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 18, 2020.

Section 23.1 of LA FOIP requires local authorities to have written policies and procedures that cover three areas: administrative, technical, and physical safeguards. All three are addressed below in more detail.

Administrative

Administrative safeguards are controls that focus on internal organization, policies, procedures, and maintenance of security measures that protect personal information. Examples include written policies and procedures, annual training for employees, confidentiality agreements, agreements with information management service providers, auditing programs, records retention and destruction schedules and access restrictions.[269]

Administrative safeguards should include, but are not limited to, having:[270]

1. A designated privacy officer

Identify an individual in your practice who will be responsible for implementing privacy policies and procedures, managing privacy breaches and being the contact for privacy inquiries and complaints.[271]

2. A privacy policy

Develop a privacy policy based on the requirements of LA FOIP as it pertains to collecting, using, and disclosing personal information, including consent requirements, individual access to information and correction and security safeguards.[272]

---

[269] SK OIPC resource, *Helpful Tips: Mobile Device Security* at p. 2.
[270] SK OIPC Investigation Report H-2011-001 at [115]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 9.
[271] SK OIPC Investigation Report H-2011-001 at [102]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 8.
[272] SK OIPC Investigation Report H-2011-001 at [113]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 8.

Develop written policies. The primary objectives of privacy and security policies are to:

- Prevent and detect malicious activities from occurring
- Assist in understanding potential security exposures and risk
- Educate, communicate, and promote security responsibilities to all stakeholders
- Comply with legislative, privacy and contractual requirements
- Identify consequences of security policy violations

If there is no documented policy, it will be difficult to communicate privacy and security practices to individuals, the public and external stakeholders, or partners. On the other hand, with a written policy in place, you are clearly demonstrating that you have done your due diligence with respect to privacy and security. This is crucial if your practice is ever subject to a privacy audit, complaint, privacy breach or security incident.[273]

Every local authority should have a privacy policy that addresses the following:

- Accountability for personal information
- Purpose for collecting personal information
- Consent for collecting, using, and disclosing personal information
- Accuracy and correction of personal information
- Retention and destruction of personal information
- Privacy breach management
- Use and disclosure audits
- Use and disclosure control
- Individual access to information
- Privacy complaint management
- Enforcement mechanisms[274]

3. Privacy procedures

Establish privacy procedures to serve as an extension of the privacy policy. Procedures should provide staff with consistent steps for managing:

- Complaints, breaches of privacy and security incidents

[273] SK OIPC Investigation Report H-2011-001 at [115]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 9.
[274] Adapted from SK OIPC Investigation Report H-2011-001 at [116].

- Individual access to and correction of personal information
- Consent[275]

Written procedures should address collection, use and disclosure practices.[276]

4. Agreements

Enter into agreements before sharing any personal information with a third party. Agreements protect employees and the organization by establishing the terms and conditions of providing personal information that it may receive from or share with others, including centralized databases and other local authorities. Agreements can also establish accountability between the local authority and electronic service providers, including network providers.[277]

If an information manager (computer support person, off-site storage company, etc.), has access to personal information, a written agreement should be in place whereby the information manager agrees to ensure confidentiality and limit access to the records.[278]

Where contracted services are used for storage, transportation, or destruction of records, including security provisions in the service contract, local authorities should require the contractors to provide a certificate of destruction.[279]

Local authorities should enforce contractual privacy provisions. A local authority's responsibilities do not end after signing a contract with an agent (i.e., contractor or

---

[275] Adapted from SK OIPC Investigation Report H-2011-001 at [135]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 8.
[276] SK OIPC Investigation Report H-2011-001 at [136].
[277] Adapted from SK OIPC Investigation Report H-2011-001 at [142]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 8.
[278] Adapted from SK OIPC Investigation Report H-2011-001 at [143]. Originates from College of Physicians and Surgeons of Saskatchewan, *Checklist for Compliance with HIPA* at p. 2.
[279] British Columbia Government Services, *FOIPPA Policy and Procedures Manual*, *Section 30 – Protection of personal information*, available at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/protection-personal-information#Unauthorized_access. Accessed June 11, 2020.

information management service provider). Rather, local authorities should monitor whether their agents are meeting the privacy requirements in their contracts. Effective monitoring entails setting dates for agents to report on their compliance, visiting agents' sites to evaluate privacy protection, meeting with agents regularly to discuss how current procedures are working and develop ways to remedy any issues and notifying agents of any changes in the local authority's own information practices that agents will be asked to adopt.[280]

All privacy requirements in a local authority's contracts with its agents should be strictly enforced. If agents refuse or fail to resolve discovered problems, court action or ending the contract may be the local authority's only options.[281]

5. A privacy awareness and education program

Local authorities should provide all staff with practical, accessible, concrete, and granular information about what they must do to comply with LA FOIP in the course of collection, use and disclosure of personal information. Four predictable problem areas are security, access, consent, and disclosure.[282]

6. Consent and communication with individuals

The best way of communicating information about privacy policies and procedures is by posting the organization's privacy policy or notice online or by providing a handout.[283]

Local authorities should identify the consent requirements under LA FOIP for any activities that involve personal information.

Consent means informed voluntary agreement by the individual with what is being done or proposed, given explicitly, either orally or in writing. *Express consent* is unequivocal and does

---

[280] SK OIPC Investigation Report H-2011-001 at [164]. Originates from *The Personal Health Information Protection Act - Implementing Best Privacy Practices*, Scott, Graham. et al., LexisNexis Butterworths: Ontario, 2005, at p. 97.
[281] SK OIPC Investigation Report H-2011-001 at [164]. Originates from *The Personal Health Information Protection Act - Implementing Best Privacy Practices*, Scott, Graham. et al., LexisNexis Butterworths: Ontario, 2005, at p. 97.
[282] SK OIPC Investigation Report H-2011-001 at [149].
[283] SK OIPC Investigation Report H-2011-001 at [156]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 8.

not require any inference on the part of the organization seeking consent; *implied consent* arises where consent may reasonably be inferred with from the action or inaction of the individual.[284]

The Local Authority Freedom of Information and Protection of Privacy Regulations requires that where consent is required by LA FOIP for the collection, use or disclosure of personal information, the consent must:

- Relate to the purpose for which the information is required
- Be informed
- Be given voluntarily
- Not be obtained through misrepresentation, fraud, or coercion
- A consent may be given that is effective for a limited period
- Consent may be express or implied unless otherwise provided
- An express consent need not be in writing[285]

7. Security protections

Ensure that reasonable and appropriate physical, administrative and technical safeguards are in place to protect personal information. Safeguards will ensure the integrity, confidentiality and availability of personal information and protect it from being improperly accessed, altered, or destroyed.[286]

Administrative safeguards, described in written policies and procedures, would also cover the following:

- That all personal information should be put away (e.g., in locked cabinets or file drawers) unless it is in use by authorized individuals. Individuals authorized to use the personal information should be clarified.

---

[284] Canadian Health Information Management Association (CHIMA), Abrams, Kelly J., Shirley Learmonth, Candace J. Gibson, *The Canadian Health Information Management Lifecycle,* 2017, at *Glossary*.
[285] *The Local Authority Freedom of Information and Protection of Privacy Regulations*, RRS c L-27.1 Reg 1, at section 11.
[286] SK OIPC Investigation Report H-2011-001 at [158]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 8.

- Personal information should not be lying around on a desk in a room where those without a need-to-know frequent.
- When file cabinets and rooms should be locked and who should have access.
- Personal information is subject to access to information requests and should be in a filing system where it is easily retrievable if required to do so.
- The training programs to make employees aware of these policies and procedures as well as LA FOIP in general.[287]

A privacy policy cannot, by itself, protect personal information held by an organization. Privacy policies that are not reflected in actual practice through strong implementation, training, and auditing will fail to safeguard personal information against privacy risks. But if we return to the true meaning of "policy," we will be reminded that it was always intended to be rooted in action. *The Concise Oxford Dictionary* defines policy as: "a course, or general plan of action adopted or proposed…"[288]

Technical

Technical safeguards mean the technology and the policy and procedures for its use to protect personal information and control access to it. Examples of technical safeguards include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital systems.[289]

Technical safeguards generally include technical security services and mechanisms.[290] General features of technical safeguards can include the following:

- Firewalls
- Encrypted transmissions with VPN technology
- Use of private keys to decrypt files

---

[287] SK OIPC Investigation Report LA-2013-003 at [82]. See also Investigation Report 200-2018 at [32].
[288] ON IPC resource, *A Policy is Not Enough: It Must be Reflected in Concrete Practices*, September 2012 at p. 1. Available at https://www.ipc.on.ca/resource/a-policy-is-not-enough-it-must-be-reflected-in-concrete-practices/.
[289] SK OIPC resource, *Helpful Tips: Mobile Device Security* at p. 2.
[290] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 134. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 18, 2020.

- Individualized passwords within an inquiry-based system limited by user roles
- Use of Oracle for backup systems
- No access to the server allowed except for domain administrators
- Data masks
- Built-in ability for process audits[291]

Electronic environments introduce several security risks. Below are some examples of technical safeguards that help eliminate and/or mitigate those risks:

- Restrict and control access to electronic files, directories, applications, databases, networks, etc. Access privileges should be based on job function and need-to-know. Regularly review and update staff access privileges.
- Ensure all users are assigned unique User IDs and passwords. Users should be authenticated every time they log on before access is granted.
- Require staff to use strong passwords (e.g., a minimum of 8 characters, use of both upper- and lower-case letters, numbers, and symbols). Passwords should be unique, difficult to guess and should not display on screen when being entered. Require staff to keep passwords confidential.
- Have computers log users out after a set period of inactivity. Implement screen savers and passwords when computers are left unattended. Ensure these features cannot be overridden by users.
- Protect networks with firewalls and anti-virus software. Monitor firewall logs to detect potential intruders. Regularly update anti-virus software.
- Initiate system audit capabilities so that access and use of electronic networks can be monitored.
- Implement user identification and strong authentication, encryption, network connection and access controls for all external connections with remote users.
- Regularly back-up electronic systems and develop and implement strict controls over back-up processes. Review backed-up information regularly to ensure it can be restored if necessary. Migrate information to new media as necessary. Provide secure off-site storage for back-ups.
- Completely delete or wipe all personal information no longer required for legal or business purposes from computer storage devices (diskettes, tapes, CD-ROMs, hard drives). If wiping is not possible, physically destroy the devices.

[291] SK OIPC Investigation Report H-2005-002 at pp. 106 to 107. Quoted again in SK OIPC Report H-2013-001 at [207].

- If the organization prints receipts for customer transactions, employ equipment that truncates or otherwise obscures credit card and debit card numbers on printouts.[292]

There is extensive information available on the appropriate management of user access privileges as they relate to personal information. One leading authority is the International Organization for Standardization (ISO). The ISO recommends the following concerning managing user access privileges:

> *Objective:* To ensure authorized user access and to prevent unauthorized access to information systems.
>
> Formal procedures should be in place to control the allocation of access rights to information systems and services.
>
> The procedures should cover all stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.
>
> …
>
> Implementation guidance
>
> The access control procedure for user registration and de-registration should include:
>
> …c) checking the level of access granted is appropriate to the business purpose (see 11.1) and is consistent with organizational security policy, e.g., it does not compromise segregation of duties (see 10.1.3);
>
> …i) periodically checking for, and removing or blocking, redundant user IDs and accounts (see 11.2.4).[293]

For some additional information on technical safeguarding, see the following SK OIPC resources:

---

[292] AB IPC resource, *Personal Information Protection Act (PIPA), PIPA Advisory #8: Implementing Reasonable Safeguards* at pp. 10 to 11.
[293] ISO Standards, *Information Technology – Security Techniques – Code of practice for information security management*, International Standard ISO/IEC 17799, (2005) at p. 61. See also SK OIPC Investigation Report F-2012-005 at [92].

Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools

Technology's Impact Upon Employee Privacy

Checklists for Trustees: Misdirected Faxes (although directed at health trustees, it may be helpful)

Faxing Personal Information and Personal Health Information: Safeguards and Responding to a Breach

Helpful Tips: Mobile Device Security

Video Surveillance Guidelines for Public Bodies

Auditing

Auditing is a technical safeguard and is necessary to assess compliance with and measure effectiveness of policies and procedures, assess compliance with legislation, assess if appropriate measures are in place to control access and monitor access.[294]

Random proactive auditing is the process of conducting an audit on a random but regular basis. Proactive auditing is the best practice and is recommended by the Commissioner.[295] Focused and targeted audits can occur in response to a privacy breach incident however proactive random auditing should be part of the organization's technical safeguards on an ongoing basis.

It is the local authority's responsibility to establish a process for conducting random audits of user activity. When developing a process for random auditing, the following can be considered:

- Who will be the individual(s) responsible for conducting random audits of user activity?
- How frequently will the random audit be conducted? Where the number of users and the volume of accesses are great, the frequency of monitoring should increase.
- How many users should be randomly audited each audit cycle?

[294] SK OIPC Investigation Report 260-2017 at [33].
[295] SK OIPC Investigation Reports H-2010-001 at [131], F-2013-003 at [109], 131-2015 at [24], 260-2017 at [51].

- What events would trigger a focused audit (e.g., a privacy breach)?[296]

An audit log is produced when conducting a random audit (i.e., sheets of data). If the audit logs are not reviewed on a regular basis by someone that can interpret the data, the random audit is not overly useful. In Investigation Report H-2013-001, the Commissioner provided guidance on this. Although focused on the equivalent provision (section 16) of *The Health Information Protection Act*, it is helpful when considering section 23.1 of LA FOIP:

> [198] … However, my office was not provided any policies or procedures that guide the review of audit logs. Such a policy and related procedure should exist to guide the review of such audit logs. For example, what would be contained in an audit log that would cause the Privacy Coordinator to investigate whether a privacy breach has occurred? How often are audit logs produced and how often are they reviewed? How are employees informed there are audit logs being produced to track their activities and for what purposes? A policy and related procedure that clearly reflects the requirements of HIPA and guides RQRHA [former Regina Qu'Appelle Regional Health Authority] in monitoring its employees is of the utmost importance in preventing and containing any similar privacy breaches.

The use of audit logs can reassure clients that their personal information is accessed only by those who need to access it and only when appropriate. The information captured in an audit log can be provided in a report to support investigations into privacy breaches and complaints.[297]

Audit reports can be used for any or all of the following:

- "Proactive auditing" as part of user compliance monitoring
- "Reactive auditing" as evidence to support complaints or privacy breaches and security incidents investigations
- Identify opportunities for additional staff education or communication
- Supporting client requests for a report on who has accessed their information[298]

---

[296] SK OIPC & eHealth Saskatchewan joint resource, *Audit and Monitoring Guidelines for Trustees*, at p. 3.

[297] The Canadian Health Informatics Association (COACH) Guidelines, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition,* Canada's Health Informatics Association, 2020, p. 25.

[298] The Canadian Health Informatics Association (COACH) Guidelines, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition,* Canada's Health Informatics Association, 2020, p. 25.

IPC Findings

In Investigation Report H-2007-001, the Commissioner investigated a breach of privacy involving Saskatchewan Health (now the Ministry of Health). The breach involved individuals receiving unsealed or improperly sealed envelopes. The envelopes contained letters that included the personal information and personal health information of the individuals. Following an investigation, the Commissioner found that Saskatchewan Health did not have adequate safeguards in place to protect personal information/personal health information externally processed for mailing by Saskatchewan Property Management (SPM). One of the Commissioner's recommendations was for Saskatchewan Health to ensure that SPM's mail processing systems and procedures were audited to determine why some envelopes would not seal properly. Further, that once this was completed, ensure that the necessary short- and long-term strategies identified through the process were implemented.

In Investigation Report H-2010-001, the Commissioner investigated a privacy breach involving L & M Pharmacy and the unauthorized viewing of personal health information in the Pharmaceutical Information Program (PIP). The Commissioner found that L & M Pharmacy was responsible for the actions of its employee. The Commissioner further found that L & M Pharmacy breached *The Health Information Protection Act* (HIPA) in several respects, chiefly by failing to adopt policies and procedures to protect the personal health information in its custody or control as required by section 16 of HIPA (equivalent provision to section 23.1 of LA FOIP). The viewing of the drug profiles of individuals was a "collection" of personal health information under HIPA that was improper. The Commissioner recommended that the User privileges of the pharmacist be suspended until L & M Pharmacy implemented appropriate policy and procedures. Further, the Commissioner recommended that the pharmacist's use of PIP, once User status is restored, be the subject of regular monthly audits by Health Information Solutions Center for one year to ensure HIPA compliance. Other recommendations were also made.

Encryption

Safeguarding personal data is essential to good information management. Not only is it essential, but it is also a legislative requirement in all access and privacy legislation throughout Canada. Personal data should be protected during all stages of collection, use

and disclosure and during retention and destruction.[299] Safeguards can include administrative (i.e., policies), physical (i.e., locks) and technical safeguards. Encryption is an example of a technical safeguard that can be used by organizations to safeguard personal data.

Encryption is the process of scrambling data (or plain text) into an unreadable form (or cipher text). This scrambling process is based on algorithms that use various forms of substitutions or transposition to encrypt the message. Algorithms are mathematical constructs that are applied through various applications to secure data transmissions or storage.[300]

Decryption is the process of using the same algorithm to restore the information into readable form.[301]

Encryption can be used at all levels of a security infrastructure. Encryption can provide confidentiality, authentication, integrity, and non-repudiation for data travelling over a network or stored on a system.[302]

There are numerous benefits to using encryption software to protect personal data. Firstly, access to personal data can be controlled both inside and outside an organization. Once encrypted, personal data can only be unlocked with a key. The key can be shared between the sender and receiver of the personal data. For electronic transmissions, encryption can be an effective way of preventing unauthorized interception of electronic messages. The sender and receiver have control over who will be permitted access. This is especially important when personal data is being sent in an email to an outside entity. Email transmission is not secure.

An unencrypted email can bounce from Toronto to Brussels to New York. It can go anywhere for that matter. It all depends on the state of Internet "traffic" that day. An email message can pass through numerous different computer systems on route to its final destination. Meanwhile, on some computers through which that email is relayed, there may be 'sniffers' or other malicious software tools. They are waiting to copy, alter or tamper with that email in

---

[299] ON IPC resource, *Encryption by Default and Circles of Trust: Strategies to Secure Personal Information in High-Availability Environments*, December 2012, at p. 2.
[300] Andress, Amanda, *Surviving Security: How to Integrate People, Process, and Technology* at Chapter 4, *Cryptography and Encryption*.
[301] Andress, Amanda, *Surviving Security: How to Integrate People, Process, and Technology* at Chapter 4, *Cryptography and Encryption*.
[302] Andress, Amanda, *Surviving Security: How to Integrate People, Process, and Technology* at Chapter 4, *Cryptography and Encryption*.

some way. Some are looking for key words or names. Other sniffers are watching for credit card numbers or login passwords.[303]

By encrypting emails before they leave the organization, it is possible to prevent unauthorized access to the personal data.

There are other benefits to using encryption. For example, the use of mobile devices in the workplace has grown exponentially over the past decade. Personal data of clients and/or customers is leaving the office on mobile devices daily. Large privacy breaches from lost or stolen work laptops, portable memory sticks and work assigned cell phones have become common. If personal data were stored in an encrypted format on the mobile device, the ability to retrieve the personal data for an improper purpose (i.e., identity theft) is significantly reduced. Breaking the code on encrypted data is not an easy task. Therefore, the more advanced the code, the more difficult it is to crack.

However, not all encryption software is created equal. Skilled hackers can find the weaknesses in encryption code or through the 'backdoors' created by many organizations as a failsafe (i.e., backdoor entry for recovery purposes). In addition, even where encryption is used on a mobile device, a hacker is likely to find clear text echoes of encrypted data left on the device. Only the use of full-drive encryption can prevent that which many organizations are not aware.[304] This is highlighted well in the Ontario Information and Privacy Commissioner's resource, *Email Encryption Made Simple*:

> Those people who use some form of encryption system relax comfortably at their keyboards. Nonetheless, they feel a cold chill each time someone reports a new security hole. Some holes are found in the encryption tools. More often though, the application that uses the encryption tool has bugs. Internet browser applications are prone to this due to their large size and complexity. While the cryptographic component might remain secure, back door bugs to the application can nullify the value of the email encryption.[305]

To assume that encryption will solve all security issues is naive. Security of personal data is an activity that requires constant diligence. Organizations should not be overly reliant on encryption software as the only form of data security. Ensuring the best and most up to date

---

[303] ON IPC resource, *E-mail Encryption Made Easy* at p. 1.
[304] Gizmo's Freeware, *Encryption is Not Enough*, available at http://www.techsupportalert.com/content/encryption-not-enough.htm, updated April 2016. Accessed June 18, 2020.
[305] ON IPC resource, *E-mail Encryption Made Easy* at p. 1.

encryption software is being used in combination with other security measures is the best approach.

IPC Findings

In Investigation Report 226-2017, the Commissioner investigated a breach of privacy involving the theft of a laptop belonging to Saskatchewan Legal Aid Commission (SLAC). The laptop contained a DVD with personal information/personal health information. The laptop was password protected but the DVD inside the laptop was not encrypted and/or password protected. SLAC received the DVD through disclosure from the Provincial Crown Prosecutor's office. The laptop, containing the DVD, was left on the front seat of a vehicle, and was not locked in a briefcase. The vehicle was left unlocked with the laptop in it all weekend. Despite having privacy policies in place regarding the transport of personal information/personal health information outside the office, the lawyer did not follow the policy. The Commissioner recommended SLAC ensure all mobile devices and storage devices that are transported outside of the office be properly encrypted and password protected. It should also be always kept with the employee in a locked briefcase.

In Investigation Report 009-2020, 053-2020, 224-2020, the Commissioner dealt with a very large data breach involving eHealth Saskatchewan, Saskatchewan Health Authority and the Ministry of Health. All three organizations were the victims of a ransomware attack in December 2019 and January 2020. The attack resulted in 40 gigabytes of data being encrypted by Ryuk ransomware and access being blocked until a ransom was paid. The ransom demand indicated a ransom needed to be paid using bitcoin to get decryption of the stolen data. No ransom was paid as there was no guarantee a copy of the data would not be kept. The data was ultimately stolen and could not be recovered. Among several recommendations, the Commissioner recommended that eHealth, the SHA and Health require cyber security training for employees and partners as the breach in this case was caused by an employee clicking on a phishing email about a job advertisement which allowed the systems to become infected.

Physical

Physical safeguards are physical measures, policies, and procedures to protect personal information and related buildings and equipment, from unauthorized intrusion and natural

and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems and clean desk approaches.[306]

Physical safeguards generally include physical standards.[307] They monitor and control the work environment. Most of these can be incorporated into every employee's work routine. Examples of physical safeguards include:

- Storing personal information in locked filing cabinets, offices, and buildings, with controls over distribution of the keys or lock combinations.
- Storing personal information in secure areas where access is limited or restricted.
- Logging out of or locking computers when stepping away from the work area.
- Ensuring that local authority assets, such as laptop computers, are secured when they are out of the office and are encrypted (e.g., not left in vehicles).
- Not leaving documents containing personal information on printers or fax machines.
- Always using a cover sheet when faxing personal information.
- Calling before sending a fax to make sure the intended recipient can retrieve it.
- Making sure the right email address has been entered prior to sending an email.
- Encrypting emails containing personal information prior to sending.
- When replying to long email threads remove any recipients who no longer need to be involved before replying.
- Limiting the amount of personal information provided in emails to that which is necessary (e.g., if everyone you are emailing knows the name of the individual being discussed, do not include the individual's name in the email).
- Shredding any documents containing personal information prior to disposal.
- Labeling files containing personal information as a reminder to store them securely.
- Card access systems, video surveillance and security guards.[308]

IPC Findings

In Investigation Report 271-2017, the Commissioner investigated a privacy breach involving the Ministry of Corrections and Policing. A Corrections Officer with the Saskatoon

[306] SK OIPC resource, *Helpful Tips: Mobile Device Security* at p. 2.
[307] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 134. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 18, 2020.
[308] Government of Newfoundland and Labrador, ATIPP Office, Department of Justice and Public Safety, *Protection of Privacy Policy and Procedures Manual,* June 2015, at pp. 73 and 74.

Correctional Centre left an inmate file on a unit's food cart and as a result, inmates were able to view the file and remove portions of the contents of the inmate's file. Further, after viewing the file contents, two inmates assaulted and killed another inmate. The Commissioner made several recommendations including that the Ministry of Corrections and Policing amend its *Code of Professional Conduct* to reflect the duty to protect personal information under the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP). The Commissioner also recommended it amend its *Oath or Declaration of Office* to include an employee's duty to protect personal information pursuant to section 24.1 of FOIP.

In Investigation Report 200-2018, the Commissioner investigated a breach of privacy involving the Saskatchewan Legal Aid Commission (SLAC). The SLAC had left its doors unlocked and wide open overnight. The Commissioner found that SLAC did not have appropriate safeguards in place to protect personal information and personal health information. This was partly since the SLAC did not have records stored in locked cabinets or locked offices at the end of the day even though cleaning staff had access to the space on a regular basis. Ultimately, it was cleaning staff that left the doors unlocked and wide open leaving the unsecured records accessible to anyone who wished to enter. Despite having a policy encouraging a clean desk, it falls short if records are not put away in locked cabinets. As such, the Commissioner found that the SLAC's practices did not go far enough to meet its obligations to protect under the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP). The Commissioner recommended that SLAC develop and implement appropriate safeguards to protect personal information and personal health information as required by section 24.1 of FOIP and section 16 of *The Health Information Protection Act*. The Commissioner indicated that this should include the use of physical safeguards, such as storing records containing personal information and personal health information in offices with locked doors or locked filing cabinets to prevent unauthorized access to these records.

Subsection 23.1(a)

Duty of local authority to protect

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

(a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;

Subsection 23.1(a) of LA FOIP requires local authorities to establish written policies and procedures that protect the integrity, accuracy and confidentiality of personal information.

Integrity refers to the condition of information being whole or complete; not modified, deleted, or corrupted.[309]

Accuracy means correct in all details.[310] Part of protecting the accuracy of personal information is ensuring the source of information can be clarified and all access, disclosure and changes can be tracked and audited.[311]

Confidentiality implies a trust relationship between the person supplying information and the individual or organization collecting it. The relationship is built on the assurance that the information will only be used by or disclosed to authorized persons or to others with the individual's permission. Protecting the confidentiality of personal information implies that individually identifying personal information is concealed from all but authorized parties.[312]

Threats to the security of information include threats to its integrity, accuracy and confidentiality. Common threats are:

---

[309] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 135. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 18, 2020.
[310] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 9, (Oxford University Press).
[311] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 145. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 19, 2020.
[312] Adapted from Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 134. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 18, 2020.

- Disclosure of information – e.g., unauthorized verbal disclosure, leaving information displayed on a monitor, electronic interception of information travelling over a transmission line, such as a fax machine or cellular phone, faxing information to the wrong fax number.
- Service interruption – e.g., power failure, labour dispute, denial of service attack on an Internet server.
- Misuse of information – e.g., transfer of or sale of personal information in contravention of LA FOIP.
- Information not being available – e.g., records that are misdirected or misfiled, or that are destroyed in a manner that is not in accordance with approved records retention and disposition schedules or policies.[313]

Local authorities should determine the likelihood (low, medium, or high) of each or any of the above threats occurring. Identify the potential consequences and rate the seriousness (less serious, serious, or very serious) of the events if they were to occur.[314]

IPC Findings

In Investigation Report 077-2014, the Commissioner investigated a breach of privacy involving the former Cypress Regional Health Authority (CRHA). The breach involved CRHA nurses and paramedics being asked to "strip charts" that contained personal health information of patients. The purpose of the stripping was to eliminate duplicate and outdated copies of personal health information for preparation of a new integrated facility and for possible scanning into the electronic medical record. The Commissioner reviewed the CRHA's directions for the staff that were stripping and found that the instructions were vague and did not offer the most basic of explanations. Further, it did not emphasize the need for the protection against unauthorized access, use and disclosure during the project or refer to safeguards that would have helped. The Commissioner found that by giving vague and inconsistent instructions to its employees, the integrity of the personal information was put at

[313] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 318. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.
[314] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 318. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.

risk. As such, the Commissioner found the CRHA did not comply with subsection 16(a) of *The Health Information Protection Act* (the equivalent to subsection 23.1(a) of LA FOIP).

Subsection 23.1(b)

Duty of local authority to protect

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

...

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the personal information in its possession or under its control;

(ii) loss of the personal information in its possession or under its control; or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control;

Subsection 23.1(b) of LA FOIP requires local authorities to establish written policies and procedures that protect against any reasonably anticipated threat or hazard to the security or integrity of personal information, loss of the personal information or against unauthorized access to or use, disclosure or modification of the personal information.

Subsection 23.1(b)(i)

Duty of local authority to protect

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

...

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the personal information in its possession or under its control;

Subsection 23.1(b)(i) of LA FOIP requires local authorities to establish written policies and procedures that protect against any reasonably anticipated threat or hazard to the security or integrity of personal information.

Reasonably anticipated

> "Reasonable" means what a reasonable person would consider appropriate in the circumstances.[315] This standard acknowledges that reasonable "does not mean perfect".[316]
>
> To "anticipate" means to be aware of (a future event) and take action; regard as probable; look forward to; to act or happen before.[317]

Threat means the possibility of trouble or danger.[318]

Hazard means a danger or risk.[319]

Security means a condition of safety or freedom from fear or danger. In the context of personal information, it refers to the physical, technological, or administrative arrangements that persons or organizations use to prevent individually identifying personal information from being altered, lost, or disclosed without authority.[320]

Integrity refers to the condition of information being whole or complete; not modified, deleted, or corrupted.[321]

Common threats are:

---

[315] British Columbia's *Personal Information Protection Act*, SBC 2003, c 63 at section 2 and subsection 4(1). See also section 2 of Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5 and the joint resource by the Service Alberta and Alberta IPC titled, *A Guide for Businesses and Organizations on the Personal Information Protection Act* at p. 9.
[316] BC IPC Investigation Report F06-01 at [49].
[317] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 57, (Oxford University Press).
[318] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 1492, (Oxford University Press).
[319] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 654, (Oxford University Press).
[320] Adapted from Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 135. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 18, 2020.
[321] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 137. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 18, 2020.

- Disclosure of information – e.g., unauthorized verbal disclosure, leaving information displayed on a monitor, electronic interception of information travelling over a transmission line, such as a fax machine or cellular phone, faxing information to the wrong fax number.
- Service interruption – e.g., power failure, labour dispute, denial of service attack on an Internet server.
- Modification of data – e.g., malicious code, forgery, addition of data to a record.
- Accidental or deliberate loss of data – e.g., physical damage to hardware, willful destruction of recorded information, information destroyed in a flood or fire.
- Misuse of information – e.g., transfer of or sale of personal information in contravention of LA FOIP.
- Information not being available – e.g., records that are misdirected or misfiled, or that are destroyed in a manner that is not in accordance with approved records retention and disposition schedules or policies.[322]

Local authorities should determine the likelihood (low, medium, or high) of each or any of the above threats occurring. Identify the potential consequences and rate the seriousness (less serious, serious, or very serious) of the events if they were to occur.[323]

In considering reasonably anticipated threats or hazards, it is exceedingly unlikely that a local authority will be in compliance with subsection 23.1(b)(i) of LA FOIP if it does not have:

- A specifically tasked privacy officer with a clear mandate and appropriate training.
- Extensive training of staff in LA FOIP requirements and provisions.
- Comprehensive, clear and practical written policies and procedures that are reinforced through leadership and training of staff.
- Written contracts with information management service providers (IMSPs) that specifically address the requirements of section 23.1 of LA FOIP.
- Audit of use and disclosures of personal information.
- Effective enforcement action to follow any breach.[324]

---

[322] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 318. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.
[323] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 318. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.
[324] Adapted from SK OIPC Investigation Report H-2011-001 at [92].

Subsection 23.1(b)(ii)

Duty of local authority to protect

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

…

(b) protect against any reasonably anticipated:

…

(ii) loss of the personal information in its possession or under its control; or

Subsection 23.1(b)(ii) of LA FOIP requires local authorities to establish written policies and procedures that protect against any reasonably anticipated loss of personal information.

Reasonably anticipated

"Reasonable" means what a reasonable person would consider appropriate in the circumstances.[325] This standard acknowledges that reasonable "does not mean perfect".[326]

To "anticipate" means to be aware of (a future event) and take action; regard as probable; look forward to; to act or happen before.[327]

Loss means the failure to maintain possession of personal information.[328]

Loss can include:

- Accidental or deliberate loss of data – e.g., physical damage to hardware, willful destruction of recorded information, information destroyed in a flood or fire.
- The removal of equipment – e.g., theft of a laptop or file containing personal information, use of information outside the office (e.g., using the information on a home computer), disposal of information at the employee's home.

---

[325] British Columbia's *Personal Information Protection Act*, SBC 2003, c 63 at section 2 and subsection 4(1). See also section 2 of Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5 and the joint resource by the Service Alberta and Alberta IPC titled, *A Guide for Businesses and Organizations on the Personal Information Protection Act* at p. 9.
[326] BC IPC Investigation Report F06-01 at [49].
[327] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 57, (Oxford University Press).
[328] Adapted from Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1132.

- Information not being available – e.g., records that are misdirected or misfiled, or that are destroyed in a manner that is not in accordance with approved records retention and disposition schedules or policies.[329]

Local authorities should determine the likelihood (low, medium, or high) of each or any of the above threats occurring. Identify the potential consequences and rate the seriousness (less serious, serious, or very serious) of the events if they were to occur.[330]

Subsection 23.1(b)(iii)

Duty of local authority to protect

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

...

(b) protect against any reasonably anticipated:

...

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

Subsection 23.1(b)(iii) of LA FOIP requires local authorities to establish written policies and procedures that protect against any reasonably anticipated unauthorized access, use or disclosure or unauthorized modification of personal information.

[329] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 318. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.
[330] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 318. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.

Reasonably anticipated

"Reasonable" means what a reasonable person would consider appropriate in the circumstances.[331] This standard acknowledges that reasonable "does not mean perfect".[332]

To "anticipate" means to be aware of (a future event) and take action; regard as probable; look forward to; to act or happen before.[333]

Unauthorized access

Access to personal information is unauthorized if an employee of a local authority does not have approved access according to the security access chart (i.e., if the employee has access to personal information which they do not need to see or handle in the course of their job duties).[334]

Unauthorized use

Use of personal information is unauthorized if it is not in accordance with section 27 (Use of personal information) of LA FOIP.[335]

---

[331] British Columbia's *Personal Information Protection Act*, SBC 2003, c 63 at section 2 and subsection 4(1). See also section 2 of Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5 and the joint resource by the Service Alberta and Alberta IPC titled, *A Guide for Businesses and Organizations on the Personal Information Protection Act* at p. 9.
[332] BC IPC Investigation Report F06-01 at [49].
[333] Pearsall, Judy, *Concise Oxford Dictionary*, 10th Ed. at p. 57, (Oxford University Press).
[334] British Columbia Government Services, *FOIPPA Policy and Procedures Manual*, *Section 30 – Protection of personal information*, available at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/protection-personal-information#Unauthorized_access. Accessed June 11, 2020.
[335] British Columbia Government Services, *FOIPPA Policy and Procedures Manual*, *Section 30 – Protection of personal information*, available at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/protection-personal-information#Unauthorized_access. Accessed June 11, 2020.

Unauthorized disclosure

An unauthorized disclosure is revealing, exposing, showing, providing copies of, selling, giving, or telling personal information in a way that is not in accordance with section 28 (Disclosure of personal information) of LA FOIP.[336]

Unauthorized modification

Is the act of making changes to personal information without authorization.[337] Unauthorized modification may occur unintentionally, through malicious code, forgery, or the wrongful addition of information to a record containing personal information.[338]

Common threats are:

- Unauthorized access – e.g., a private business receives numerous faxes in error from the Saskatchewan Health Authority. The faxes were intended for a physician and contain personal health information of patients. It was found the only difference between the telephone numbers was one digit.[339]
- Unauthorized use – e.g., employees using their access privileges to view the information of a co-worker (i.e., snooping) in electronic systems for a purpose other than what it was collected for is an unauthorized use.[340]
- Unauthorized disclosure – e.g., unauthorized verbal disclosure, leaving information displayed on a monitor, electronic interception of information travelling over a transmission line, such as a fax machine or cellular phone, faxing information to the wrong fax number.
- Unauthorized modification - malicious code, forgery, addition of data to a record.

---

[336] British Columbia Government Services, *FOIPPA Policy and Procedures Manual*, *Section 30 – Protection of personal information*, available at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/protection-personal-information#Unauthorized_access. Accessed June 11, 2020.
[337] Adapted from Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 916.
[338] Adapted from Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 136. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 18, 2020.
[339] SK OIPC Investigation Report 043-2018 at [25] and [26].
[340] SK OIPC Investigation Report H-2013-001 at [41] and [42].

- Misuse of information – e.g., transfer of or sale of personal information in contravention of LA FOIP.[341]

Local authorities should determine the likelihood (low, medium, or high) of each or any of the above threats occurring. Identify the potential consequences and rate the seriousness (less serious, serious, or very serious) of the events if they were to occur.[342]

Subsection 23.1(c)

Duty of local authority to protect

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

...

(c) otherwise ensure compliance with this Act by its employees.

It is expected that a local authority will have appropriate safeguards in place to protect personal information.[343] Local authorities should have **written** policies and procedures in place to guide employees with what is required by law concerning privacy protection for personal information. Without written policies and procedures, a local authority has not taken reasonable steps to safeguard personal information in its possession or control.[344]

Local authorities are responsible for taking steps to ensure that its officers and staff comply with the protection of privacy requirements under LA FOIP. This involves:

- Ensuring that policies and procedures that safeguard personal information are in place,
- That officers and staff are aware and understand the policies and procedures; and

[341] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 318. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.
[342] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 318. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.
[343] SK OIPC Investigation Report 200-2018 at [34].
[344] SK OIPC Investigation Reports H-2011-001, F-2007-001 at [48] and LA-2013-003 at [54] to 57].

- Are provided privacy training.

Comply with means to act in accordance with or fulfil the requirements.[345]

If there is no documented policy, it will be difficult to communicate privacy and security practices to staff. On the other hand, with a written policy in place, a local authority is clearly demonstrating that it has done its due diligence with respect to privacy and security. This is crucial if the local authority's practices are ever subject to a privacy audit, complaint, privacy breach or security incident.[346]

Every local authority should have a privacy policy that addresses the following:

- Accountability for personal information.
- Purpose for collecting personal information.
- Consent for collecting, using, and disclosing personal information.
- Accuracy and correction of personal information.
- Retention and destruction of personal information.
- Privacy breach management.
- Use and disclosure audits.
- Use and disclosure control.
- Individual access to information.
- Privacy complaint management.
- Enforcement mechanisms.[347]

It should also have privacy procedures that provide staff with consistent steps for managing:

- Complaints, breaches of privacy and security incidents.
- Individual access to and correction of personal information.
- Consent.[348]

---

[345] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[346] SK OIPC Investigation Report H-2011-001 at [115]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition* at p. 9.
[347] Adapted from SK OIPC Investigation Report H-2011-001 at [116].
[348] Adapted from SK OIPC Investigation Report H-2011-001 at [135]. Originates from Canada's Health Informatics Association, *Putting it into Practice: Privacy and Security for Healthcare Providers*

Section 23.2: Information Management Service Provider

Information management service provider

23.2(1) A local authority may provide personal information to an information management service provider for the purposes of:

(a) having the information management service provider process, store, archive or destroy the personal information for the local authority;

(b) enabling the information management service provider to provide the local authority with information management or information technology services;

(c) having the information management service provider take possession or control of the personal information;

(d) combining records containing personal information; or

(e) providing consulting services.

(2) Before disclosing personal information to an information management service provider, a local authority shall enter into a written agreement with the information management service provider that:

(a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the personal information;

(b) provides for the protection of the personal information; and

(c) meets the requirements of this Act and the regulations.

(3) An information management service provider shall not obtain access to, use, disclose, process, store, archive, modify or destroy personal information received from a local authority except for the purposes set out in subsection (1).

(4) An information management service provider shall comply with the terms and conditions of the agreement entered into pursuant to subsection (2).

Section 23.2 of LA FOIP provides authority to a local authority to disclose personal information to an information management service provider for specific purposes outlined in the provision. An example of such a service is Crown Shred & Recycling which is a company utilized by many government institutions for record destruction services.

Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition at p. 8.

Section 23.2 of LA FOIP was a new additional provision in LA FOIP that came into force on January 1, 2018. The accompanying section 8.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* also came into force at the same time.

Much of the experience in Saskatchewan surrounding information service providers comes from work surrounding section 18 of *The Health Information Protection Act* (HIPA). However, the concept of an information management service provider is by no means unique to Saskatchewan. It is a common feature in other privacy legislation across Canada (see for example Manitoba's *The Personal Health Information Act*, Alberta's *Health Information Act*, Ontario's *Personal Health Information Protection Act*, and Newfoundland and Labrador's *Personal Health Information Act*). The title may be different, but in each of these statutes there is a specific provision for a health trustee to make arrangements for a third party to store or destroy personal health information.[349]

Subsection 23.2(1)

Information management service provider

23.2(1) A local authority may provide personal information to an information management service provider for the purposes of:

(a) having the information management service provider process, store, archive or destroy the personal information for the local authority;

(b) enabling the information management service provider to provide the local authority with information management or information technology services;

(c) having the information management service provider take possession or control of the personal information;

(d) combining records containing personal information; or

(e) providing consulting services.

Subsection 23.2(1) of LA FOIP provides that a local authority can disclose personal information in its possession or control to an information management service provider (IMSP) provided the purpose for sharing is for one of the services or functions outlined in subsection 23.2(1) of LA FOIP.

[349] SK OIPC Investigation Report H-2011-001 at [194].

An **information management service provider (or IMSP)** means a person or body that performs one or more of the functions or provides one or more of the following services to a local authority:

- Processes, stores, archives, or destroys records containing personal information (e.g., Crown Shred & Recycling)
- Provides information management or information technology services with respect to records containing personal information (e.g., Government of Saskatchewan Information Technology Services Branch, SaskBuilds and Procurement IT Division, private companies offering case file management services)[350]

An information management service provider might also do the following on behalf of a local authority:

- Combine records (e.g., merging or deleting duplicate records)
- Provide consulting services[351]

Subsection 23.2(2)

Information management service provider

23.2(2) Before disclosing personal information to an information management service provider, a local authority shall enter into a written agreement with the information management service provider that:

(a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the personal information;

(b) provides for the protection of the personal information; and

(c) meets the requirements of this Act and the regulations.

---

[350] *The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c L-27.1 at subsection 2(e.1).

[351] Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 164. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.

Before disclosing personal information to an information management service provider, a local authority must have a written agreement in place that includes the requirements outlined at subsection 23.2(2) of LA FOIP.

An **information sharing agreement** is a written record of understanding between parties that outlines the terms and conditions under which personal information is shared between the parties. An adequate information sharing agreement should be in place between the parties to protect the personal information involved and to ensure compliance.[352]

Subsection 23.2(2) of LA FOIP sets out specific requirements that must be in an information sharing agreement between a local authority and an information management service provider. The agreement must address:

- The access to, use, disclosure, storage, archiving, modification and destruction of personal information (s. 23.2(2)(a))
- The protection of personal information (s. 23.2(2)(b))
- The requirements of LA FOIP and *The Local Authority Freedom of Information and Protection of Privacy Regulations* (LA FOIP Regulations). Specifically, section 8.2 of the LA FOIP Regulations which provides:

> **Agreement between local authority and information management service provider**
>
> **8.2** For the purposes of clause 23.2(2)(c) of the Act, a written agreement that is entered into between a local authority and an information management service provider must include:
>
> (a) a description of the specific service the information management service provider will deliver;
>
> (b) provisions setting out the obligations of the information management service provider respecting the security and safeguarding of personal information; and
>
> (c) provisions for the destruction of the personal information, if applicable.

[352] Government of Canada, Treasury Board of Canada Secretariat resource, *Guidance on Preparing Information Sharing Agreements Involving Personal Information*. Available at https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html. Updated July 2010. Accessed June 23, 2020.

In addition to what LA FOIP and the LA FOIP Regulations require in an information management sharing agreement, there are also some best practices to keep in mind. A well written agreement should also include:

- Identities, roles, and responsibilities of the parties.
- What information is being disclosed and collected and the purpose(s) of each.
- The frequency and duration of information exchanged.
- The legal authority to disclose and collect information.
- The methods and security measures for transferring and storing the information.
- Procedures in the event there is a privacy or security breach.
- Limitations for collection, use, disclosure, and retention.
- Provisions for accuracy of the information.
- Indemnification.
- Compliance monitoring.[353]

An information management service provider must comply with the terms and conditions of the agreement. **Comply with** means to act in accordance with or fulfil the requirements.[354]

LA FOIP does not prohibit the transfer of personal information to outside of Canada. However, any local authority outsourcing personal information outside of Canada still has several obligations under LA FOIP such as ensuring safeguards are adequate, a detailed contract is in place and other provisions of LA FOIP are met.[355]

For more on best practices and developing information sharing agreements, see SK OIPC resource, *Best Practices for Information Sharing Agreements*.

For resources from other jurisdictions on information sharing agreements see:

The Office of the Newfoundland and Labrador Information and Privacy Commissioner, *Information Sharing Agreements: Essential Administrative Safeguards*.

The Government of Canada's *Guidance on Preparing Information Sharing Agreements Involving Personal Information*.

---

[353] SK OIPC resource, *Best Practices for Information Sharing Agreements* at p. 4. Originates from the Institute for Citizen-Centered Service resource, *Guidelines for Best Practice*.
[354] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[355] For more on requirements when outsourcing personal information outside of Canada, see SK OIPC Investigation Report F-2013-001.

Service Alberta, *Guide for Developing Personal Information Sharing Agreements*.

IPC Findings

In Investigation Report 072-2018, the Commissioner considered the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP) for the first time. The Commissioner investigated the Ministry of Central Services' (Central Services) use of backup tape technology and the potential issues posed by this technology. The Commissioner found that Central Services had an agreement in place with Information Management Services (ISM) but had not been reviewed since the new requirements were added to FOIP on January 1, 2018. Further, the Commissioner found that there was no agreement in place between ISM and a subcontractor. The Commissioner recommended that Central Services review the existing contract with ISM to ensure it complies with section 24.2 of FOIP. Additionally, the Commissioner recommended that Central Services require ISM and the subcontractor to have a written agreement in place that was compliant with section 24.2 of FOIP.

Subsection 23.2(3)

Information management service provider

23.2(3) An information management service provider shall not obtain access to, use, disclose, process, store, archive, modify or destroy personal information received from a local authority except for the purposes set out in subsection (1).

Subsection 23.2(3) of LA FOIP provides that an information management service provider shall not access, use, disclose, process, store, archive, modify or destroy personal information received from a local authority except for the purposes outlined at subsection 23.2(1) of LA FOIP.

The purposes set out in subsection 23.2(1) of LA FOIP include:

- Processing, storing, archiving, or destroying personal information
- Information management or information technology services
- Combining records (e.g., merging or deleting duplicate records)

- Consulting services[356]

Subsection 23.2(4)

Information management service provider

23.2(4) An information management service provider shall comply with the terms and conditions of the agreement entered into pursuant to subsection (2).

Subsection 23.2(4) of LA FOIP provides that an information management service provider shall comply with the terms of the agreement entered into with the local authority pursuant to subsection 23.2(2) of LA FOIP.

It is best practice to monitor the effectiveness of any agreement. This is done through audit trails, self-assessments, audits, verification systems, certificates of assurance and measurement techniques related to the local authority's obligations in the agreement.[357]

Recognizing that it is not enough to rely on contractors to self-report their breaches, a local authority that has entered into an outsourcing contract should create and implement a program of regular, thorough compliance audits. Such audits should be performed by a third party auditor, selected by the local authority, that has the necessary expertise to perform the audit and recommend any necessary changes and mitigation measures. Consideration should be given to providing that the contractor must pay for any audit that uncovers material noncompliance with the contract.[358]

---

[356] *The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c L-27.1 at section 23.2(1). See also Government of Alberta, *Health Information Act, Guidelines and Practices Manual*, March 2011 at p. 164. Available at https://open.alberta.ca/dataset/50877846-0fba-4dbb-a99f-eeb651533bc4/resource/3e16d527-2618-48ae-80b8-93f69973878e/download/hia-guidelines-practices-manual.pdf. Accessed June 23, 2020.

[357] SK OIPC resource, *Best Practices for Information Sharing Agreements* at p. 4. Originates from the Institute for Citizen-Centered Service resource, *Guidelines for Best Practice*.

[358] SK OIPC Investigation Report F-2013-001 at [107]. Originates from BC IPC *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*, October 2004, at p. 20.

Section 24: Purpose of Information

Purpose of information

24 No local authority shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the local authority.

Section 24 establishes the rules under which a local authority can collect personal information.

Collection means to bring or come together; assemble; accumulate; obtain personal information from any source by any means.[359]

Collection occurs when a local authority gathers, acquires, receives, or obtains personal information. It includes the gathering of information through forms, interviews, questionnaires, surveys, polls, and video surveillance. There is no restriction on how the information is collected. The means of collection may be in writing, audio or videotaping, electronic data entry or other means.[360] Viewing personal information is also a collection.[361] Collection can mean examining personal information, recording, or photocopying it. Although each form of collection is not equal or interchangeable, each represent a collection with its own inherent privacy challenges.[362] Collection does not require that the information be recorded immediately or within a certain period of time. It is conceivable that one can view or hear any matter of information through the day and later recall it and proceed to record it.[363]

When challenged on its collection of personal information, a local authority must be able to demonstrate that the collection of personal information was for a specific purpose, necessary and lawful in accordance with sections 24 and 25 of LA FOIP.

---

[359] SK OIPC *2009-2010 Annual Report* at *Appendix I, Definitions*, p. 53. See also British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[360] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 236.
[361] SK OIPC Investigation Reports F-2013-003 at [25], H-2010-001 at [89], 282-2016 at [10], 199-2019 at [23]. See also PEI IPC Investigation Report No. PP-20-001 at [33] and AB IPC Order H2007-002 at [72], [89] and [90].
[362] AB IPC news release, *Collection of Driver's Licence Numbers Under Privacy Sector Privacy Legislation* (December 8, 2008). See also SK OIPC Investigation Report 199-2019 at [22].
[363] SK OIPC Investigation Report 199-2019 at [23].

Purpose means the purpose for which personal information was obtained or compiled, the object to be attained or the thing intended to be done, e.g., the administration of a program, the provision of a service or other activity.[364] The purpose of a collection means the reason(s) the personal information is needed and the use(s) that the local authority will make of the personal information.[365]

Relates to should be given a plain but expansive meaning.[366] The phrase should be read in its grammatical and ordinary sense. There is no need to incorporate complex requirements (such as "substantial connection") for its application, which would be inconsistent with the plain unambiguous meaning of the words of the statute.[367] "*Relating to*" requires a purpose with some connection to an existing or proposed program or activity of the local authority.[368]

Existing means that the program or activity must be in place at the time the personal information is collected.[369]

Proposed means something offered for consideration or acceptance; a suggestion.[370] To put forward an idea or plan for consideration.[371] In this context, it means the personal information was collected for a purpose relating to a program that is at the stage of being proposed but not yet existing.

Program means formally recognized activities or functions designed to deliver specific services that are related to a specific subject matter or topic. Programs do not refer to computer programs.[372]

---

[364] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[365] SK OIPC Investigation Report F-2012-001 at [62]. Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 248.
[366] *Gertner v. Lawyers' Professional Indemnity Company,* 2011 ONSC 6121 (CanLII) at [32].
[367] Adapted from *Ministry of Attorney General and Toronto Star*, 2010 ONSC 991 (CanLII) at [45].
[368] Adapted from *Ministry of Attorney General and Toronto Star*, 2010 ONSC 991 (CanLII) at [43].
[369] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-46. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_6.pdf. Accessed on June 29, 2020.
[370] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1474.
[371] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 1147.
[372] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Activity is an individual action designed to assist in carrying out an operating program. For example:

- Skills training assists a social assistance recipient to return to the workforce and is one facet of the social assistance program.
- Driver testing is required in determining eligibility for a driver's licence as part of the driver-licensing program.[373]

The local authority must have a demonstrable need for the personal information such that the operating program or activity would not be viable without it.[374]

Though the principle of "minimal collection" is not expressly referred to in the legislation, it is a tenet of LA FOIP that a local authority should collect only the minimum amount of personal information necessary for the intended program or activity. Local authorities should have administrative controls in place to ensure that they do not collect any more personal information than is necessary for the related programs or activities. They must have legislative authority for the relevant program or activity, and a demonstrable need for each piece of personal information collected in order to carry out the program or activity.[375] For more on this, see *Data Minimization* earlier in this Chapter.

As part of its general objective of limiting the amount of personal information that local authorities may accumulate and make use of, LA FOIP contains specific restrictions on the authority of local authorities to collect personal information. These restrictions limit both the purposes for which local authorities may collect personal information and the manner in which such information may be collected.[376]

---

[373] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[374] SK OIPC Investigation Report F-2012-001 at [18]. See also Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 237.
[375] SK OIPC Investigation Report F-2012-001 at [20] and [21]. Originally drawn from Treasury Board of Canada Secretariat, *Guidance on Preparing Information Sharing Agreements Involving Personal Information* (July 2010), available at https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html.
[376] SK OIPC Investigation Report F-2012-001 at [19]. Originated from K. Klein and D. Kratchanov: *Government Information: The Right to Information and the Protection of Privacy in Canada*, Second Edition (Toronto: Carswell Press, 2009) at pp. 8-15.

In general terms, LA FOIP limits the entitlement of local authorities to personal information so that they may only collect such information to the extent that it is necessary or relevant to the various lawful activities of the local authority. Moreover, local authorities may only collect personal information in certain permitted ways which have the effect of giving notice that the information is in fact being collected by a local authority and indicating the general reason for it being collected (see section 25 below for more).[377]

IPC Findings

In Investigation Report F-2012-001, the Commissioner considered the over collection of a customer's personal information by Saskatchewan Telecommunications (SaskTel) as part of its identity verification process. The Commissioner found that SaskTel did not have authority to collect the Saskatchewan Health Services Number. Secondly, SaskTel did not provide a satisfactory explanation as to why it needed to collect other unique identifiers over the telephone since it could not verify the accuracy of same. Thirdly, the Commissioner found that SaskTel was collecting third party personal information without authority. Further, the Commissioner found that SaskTel was not meeting the notice requirements of subsection 26(2) of *The Freedom of Information and Protection of Privacy Act* (FOIP) – equivalent to subsection 25(2) of LA FOIP. The Commissioner recommended that SaskTel conduct a privacy impact assessment, revise its privacy policy and prepare a script to ensure that its customers understand what is optional when providing proof of identity. The Commissioner further recommended that SaskTel purge its systems of all personal information and personal health information of its customers and third parties that it collected without the requisite authority within 60 days.

Over collection

Over collection is where a local authority collects more personal information than is necessary to accomplish the authorized purpose.[378]

---

[377] SK OIPC Investigation Report F-2012-001 at [19]. Originated from K. Klein and D. Kratchanov: *Government Information: The Right to Information and the Protection of Privacy in Canada*, Second Edition (Toronto: Carswell Press, 2009) at pp. 8-15.

[378] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-52. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_6.pdf. Accessed on July 15, 2020.

Local authorities must take care to limit both the type and amount of personal information collected to that which is necessary to fulfill the identified purposes. Local authorities should also be specific about what kind of personal information it needs to collect.[379]

An example of over collection could be where an individual making an injury insurance claim following a motor vehicle accident is asked to disclose their entire personal health history in order to have their injury claim assessed even though the entire personal health history may not be relevant.[380]

Local authorities that over collect personal information run a higher risk of dealing with privacy breaches due to holding on to too much personal information on individuals. Large quantities of personal information require ongoing safe storage, secure access, proper destruction and continued compliance regarding use and disclosure. It is not in a local authority's interest to over collect personal information. It also makes individuals more vulnerable to a complete loss of control over their personal information. For example, when identity theft occurs. Most importantly, it is not authorized under LA FOIP. The principle of data minimization must be abided by. For more on this, see *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report F-2013-002, the Commissioner investigated a complaint that related to the over collection of personal information and personal health information by Saskatchewan Government Insurance (SGI). The Complainant alleged the collection of personal information and personal health information by SGI for purposes of processing her injury claim was excessive. SGI collected the Complainant's entire medical file from her physician instead of collecting only information pertaining to her neck and back from 2004 to 2008. When the Commissioner initiated an investigation, SGI took the position that the Commissioner did not have jurisdiction to investigate the matter as the matter concerned the collection of medical information under Part VIII of *The Automobile Accident Insurance Act* (AAIA). SGI also asserted that the collection of the Complainant's personal information and personal health information was authorized pursuant to section 165 of *The Automobile Accident Insurance Act* and that a consent form was signed by the Complainant authorizing

[379] Office of the Privacy Commissioner of Canada, *Investigation into authentication and transfer practices used during Loblaw gift card offering,* PIPEDA Report of Findings # 2019-003, October 16, 2019.
[380] For the history of this example, see SK OIPC Investigation Reports H-2004-001, F-2010-001 and F-2013-002.

the collection. Upon investigation, the Commissioner found that FOIP applied, and that the Commissioner had jurisdiction to investigate the matter. The Commissioner also found that although the Complainant signed a consent form, there were issues with the consent form. The consent form appeared to allow SGI to collect any and all information in order to adjudicate an injury claim. The Commissioner also found that SGI over collected the Complainant's personal information and personal health information in this matter. The Commissioner recommended that SGI not use the consent form because it confused claimants by allowing them to think they had some measure of control over the collection of their personal information when in fact SGI had authority to collect personal information without consent under the AAIA. Alternatively, the Commissioner recommended that if SGI chose to continue using the misleading consent form, that it respects the need-to-know and data minimization principles and not collect personal information or personal health information that was not needed or relevant for processing an injury claim.

In Investigation Report 212-2016, the Commissioner investigated a complaint alleging that the Ministry of Social Services (MSS) over collected an individual's personal information. The Complainant was concerned with MSS wanting to know where she shopped for her groceries in order to receive social assistance benefits, querying numerous financial institutions to determine if she held any accounts with them, and viewing a business bank account of the Complainant from 2014. MSS provided its reasoning to the Commissioner for collecting the personal information. It indicated that individuals must provide sufficient documentation to validate that they meet the eligibility criteria for income assistance. Upon investigation, the Commissioner found that the Complainant had signed a consent form allowing MSS to collect her personal information, so MSS had authority to collect the Complainant's personal information. The Commissioner also found that MSS did not over collect the Complainant's personal information. The Commissioner recommended that MSS modify its consent form to be clearer for individuals what will be collected and from where.

Unsolicited Information

An individual may submit personal information on their own initiative without the information being requested by a local authority. Receipt of this information is not considered a collection unless the local authority keeps or uses the information.[381] In other

[381] Ministry of Government and Consumer Services, Information, Privacy and Archives, *Freedom of* Ontario *Information and Protection of Privacy Manual* at p. 140. Available at https://files.ontario.ca/books/foi_privacy_manual_-_final-v02-2018-03-08-en-accessible.pdf. Accessed December 1, 2022. See also SK OIPC Investigation Reports F-2012-002 at [61] and F-2012-004 at [77].

words, if the local authority keeps it, it should ensure it has authority to do so under section 24 of LA FOIP. If not, return it or safely destroy it.

If a local authority does not have specific authority to collect unsolicited personal information and the information is not necessary for an operating program or activity of the local authority, it is not an authorized collection. The local authority should adopt a policy of either returning the unsolicited information or destroying it in accordance with a transitory records schedule.[382]

In some cases, a local authority might keep unsolicited personal information for a specified period before destroying it (e.g., unsolicited resumes). The local authority should keep the unsolicited personal information separate from other files so that it will not be improperly used or disclosed.[383]

IPC Findings

In Investigation Report F-2012-002, the Commissioner investigated a complaint concerning the Saskatchewan Workers' Compensation Board (WCB). The complaint concerned the disclosure of an individual's personal information to a third party trucking company, specifically, that the individual had a claim with WCB. The Commissioner found that there was an unauthorized disclosure by the WCB to the third party trucking company when it confirmed the individual had an active WCB claim. The Commissioner also found that during the conversation between WCB and the trucking company, WCB collected personal information of the individual without proper authority to do so under section 25 of *The Freedom of Information and Protection of Privacy Act* (FOIP) – equivalent to subsection 24 of LA FOIP.

[382] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 239. See also SK OIPC Investigation Report F-2012-002 at [60].
[383] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 240. See also SK OIPC Investigation Report F-2012-002 at [60].

Section 25: Manner of Collection

Manner of collection

25(1) A local authority shall, where reasonably practicable, collect personal information directly from the individual to whom it relates.

(2) A local authority that collects personal information that is required by subsection (1) to be collected directly from an individual shall, where reasonably practicable, inform the individual of the purpose for which the information is collected.

(3) Subsections (1) and (2) do not apply where compliance with them might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected.

Subsection 25(1): Direct Collection

Manner of collection

25(1) A local authority shall, where reasonably practicable, collect personal information directly from the individual to whom it relates.

Subsection 25(1) of LA FOIP requires that a local authority shall, where reasonably practicable, collect personal information directly from the subject individual. Only one exception is provided for at subsection 25(3) of LA FOIP.

Collection means to bring or come together; assemble; accumulate; obtain personal information from any source by any means.[384]

Reasonably practicable:

Reasonable means fair, proper or moderate under the circumstances, sensible.[385]

---

[384] SK OIPC *2009-2010 Annual Report* at *Appendix 1, Definitions* at p. 53. See also British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

[385] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 1456.

Practicable means feasible, fair, and convenient and is not synonymous with possible. An act is practicable of which conditions or circumstances permit the performance.[386]

What is reasonably practicable depends on the circumstances in each case.

Directly means straight, undeviating.[387]

The "direct collection" requirement is an important aspect of the "Openness" privacy principle (see Principle #8 of the *10 Fair Information Principles* earlier in this Chapter). It is intended to ensure that an individual is generally aware of the personal information that a local authority is collecting about them. To exercise the privacy rights under Part IV of LA FOIP, such as the right to request a correction of personal information or to complain if the information is being used or disclosed in a manner not authorized by LA FOIP, an individual must have some idea as to the nature of the personal information being collected about them.[388]

Subsection 25(2): Inform Individual

Manner of collection

25(2) A local authority that collects personal information that is required by subsection (1) to be collected directly from an individual shall, where reasonably practicable, inform the individual of the purpose for which the information is collected.

Subsection 25(2) of LA FOIP provides that where a local authority is collecting personal information from an individual directly, it must, where reasonably practicable, inform the individual of the purpose for which the information is being collected. Presently, there is only one exception provided for to this general rule in LA FOIP. The one exception is subsection 25(3) of LA FOIP which permits indirect collection for specific reasons. Where subsection 25(3) of LA FOIP applies, informing the individual would be counterproductive and is therefore not required. For more on subsection 25(3) and some examples of where this could apply, see *Subsection 25(3)*, later in this Chapter.

---

[386] Gardner, J., and Gardner K. (2016) *Sangan's Encyclopedia of Words and Phrases Legal Maxims*, Canada, 5th Edition, Volume 4, P to R, at p. P-280. The Court of Appeal of Alberta relied on this definition in *R. v. Mudry*, 1979 ABCA 286 (CanLII) at [14] and again in the Provincial Court of Alberta decision *R. v. Graham*, 2014 ABPC 197 (CanLII) at [14].

[387] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 576.

[388] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Appendix 1 – Glossary of Terms* at p. 13. Available at *Resource Manual | FIPPA | Province of Manitoba (gov.mb.ca)* at Chapter 6., p. 6-54. Accessed December 5, 2022.

Where it is reasonably practicable, the local authority must inform the individual of the purpose for which the information is being collected. The phrase "reasonably practicable" is not defined in LA FOIP. However, the following assists:

Reasonably practicable :

> **Reasonable** means fair, proper or moderate under the circumstances, sensible.[389]
>
> **Practicable** means feasible, fair, and convenient and is not synonymous with possible. An act is practicable of which conditions or circumstances permit the performance.[390]
>
> What is reasonably practicable depends on the circumstances in each case.

Purpose means the purpose for which personal information was obtained or compiled, the object to be attained or the thing intended to be done, e.g., the administration of a program, the provision of a service or other activity.[391] The purpose of a collection means the reason(s) the personal information is needed and the use(s) that the local authority will make of the personal information.[392]

Informing or "notification" allows individuals to understand the purpose, nature, and extent of collection of personal information. Without this information, individuals are unable to ensure that their rights under LA FOIP are respected.[393] Notification enables an individual to make an informed decision as to whether to give the personal information to the local authority, ability to understand the consequences of providing it and the ability to exercise privacy rights such as making a privacy complaint. These are at the heart of *Fair Information Principles* numbers 2 (identifying purposes) and 8 (openness). For more on these principles, see *10 Fair Information Principles* earlier in this Chapter.

---

[389] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 1456.
[390] Gardner, J., and Gardner K. (2016) *Sangan's Encyclopedia of Words and Phrases Legal Maxims*, Canada, 5th Edition, Volume 4, P to R, at p. P-280. The Court of Appeal of Alberta relied on this definition in *R. v. Mudry*, 1979 ABCA 286 (CanLII) at [14] and again in the Provincial Court of Alberta decision *R. v. Graham*, 2014 ABPC 197 (CanLII) at [14].
[391] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[392] SK OIPC Investigation Report F-2012-001 at [62]. Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 248.
[393] SK OIPC Investigation Report F-2012-001 at [61].

Notification may be given in many ways. It may be:

- Printed on a collection form.
- Contained on a separate sheet or in a brochure accompanying a form.
- Presented in a pop-up window linked to an online form.
- Published in a calendar of a post-secondary institution or an information brochure about a program that is provided to all applicants.
- Displayed on a notice hung on the wall or placed on a service counter.
- Given orally, for example, during a telephone call.[394]

A local authority must inform an individual of:

- The purpose for which the personal information is collected.
- The specific legal authority for the collection (see footnote).[395]
- The title, business address and business telephone number of an officer or employee of the local authority who can answer the individual's questions about the collection.[396]

Notification should be given at the time that the personal information is being collected.[397]

If notification is given orally, either in person or over the telephone, it is a good practice to refer the individual to a written copy of the notice or to provide a printed copy either at the counter or later by mail, and to retain a record that the notice was given.[398]

---

[394] SK OIPC Investigation Report F-2012-001 at [62]. Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 249.
[395] "Legal authority" for collection may be a specific provision in an enactment of Saskatchewan or a federal enactment that expressly authorizes collection of the personal information. It can also be authority under section 24 of LA FOIP, which authorizes collection of personal information for a purpose that relates to an existing or proposed program or activity of the local authority.
[396] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 248. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at pp. 6-91 to 6-92. Available at Chapter (gov.mb.ca). Accessed December 13, 2022.
[397] SK OIPC Investigation Report F-2012-001 at [62]. Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 249.
[398] SK OIPC Investigation Report F-2012-001 at [62]. Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 249.

Local authorities should undertake a regular review of their collection instruments to determine which ones require the inclusion of collection notices. Collection notices should be included on all print and electronic forms used to collect personal information directly.[399]

IPC Findings

In Investigation Report F-2012-001, the Commissioner considered the over collection of a customer's personal information by Saskatchewan Telecommunications (SaskTel) as part of its identity verification process. The Commissioner found that SaskTel did not have authority to collect the Saskatchewan Health Services Number. Secondly, SaskTel did not provide a satisfactory explanation as to why it needed to collect other unique identifiers over the telephone since it could not verify the accuracy of same. Thirdly, the Commissioner found that SaskTel was collecting third party personal information without authority. Further, the Commissioner found that SaskTel was not meeting the notice requirements of subsection 26(2) of *The Freedom of Information and Protection of Privacy Act* (FOIP) – equivalent to subsection 25(2) of LA FOIP. It's notification on its website was too vague to be particularly informative to customers as it made no mention of the options to provide alternative information instead of unique identifiers and other sensitive personal information. The Commissioner recommended that SaskTel conduct a privacy impact assessment, revise its privacy policy and prepare a script to ensure that its customers understand what is optional when providing proof of identity. The Commissioner further recommended that SaskTel purge its systems of all personal information and personal health information of its customers and third parties that it collected without the requisite authority within 60 days.

Subsection 25(3): Exception to Informing

Manner of collection

25(3) Subsections (1) and (2) do not apply where compliance with them might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected.

Subsection 25(3) of LA FOIP provides that subsections (1) and (2) do not apply where compliance with them might result in "the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected."

[399] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 250

This provision recognizes that in certain limited circumstances, collecting personal information directly from the individual, may result in inaccurate information being collected. For example, if a local authority is required to collect personal information directly (s. 25(1)) and notify the individual of the purpose for the collection (s. 25(2)) in advance, an individual may not be forthcoming, may provide partial information or may provide inaccurate information. Surveys seeking opinions and psychological testing are examples where this might be the case. Another example is investigations. Much personal information about a person who is under investigation is collected from other sources. Reasons for this include the fact that investigators may not wish to alert the individual concerned that an investigation is taking place, the individual would not provide accurate information, or the individual might alter or destroy evidence.[400]

To rely on this provision to collect indirectly and not provide notification to an individual, the threshold that must be met is "might result" in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected. LA FOIP does not define these terms. Based on dictionary meanings of these terms the IPC establishes the threshold as follows:

Might means a possibility.[401] "Possible" means capable of existing, happening, or being achieved; that which is not certain or probable.[402]

Might is significantly less than "probable" or "likely". "Probable" means likely to happen or be the case.[403] At the other end of the threshold is "speculation". Speculation is based on conjecture rather than knowledge. Conjecture is an opinion or conclusion based on incomplete information. Speculation generally has no objective basis.[404] Therefore, "might" is higher than *speculation* but lower than *probable*.

The word "might" speaks to possibilities. Is the prospect of collecting inaccurate information, defeating the purpose, or prejudicing the use of the personal information within the realm of possibility or beyond it?[405]

---

[400] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 244.
[401] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 902.
[402] See SK OIPC Review Report 082-2019, 083-2019 at [72] Originates from Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 1117.
[403] See SK OIPC Review Report 082-2019, 083-2019 at [73].
[404] See SK OIPC Review Report 082-2019, 083-2019 at [71]. Originates from Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at pp. 1379 and 301.
[405] *R. v. Fulton*, 2006 SKCA 115 (CanLII) at [21].

Result means a consequence, effect, or outcome.[406]

Inaccurate information is incorrect, incomplete, or misleading information, or information which does not reflect the truth.[407]

Defeat the purpose means it prevents the purpose from being achieved; to thwart or frustrate.[408]

Prejudice the use in this context refers to detriment to the ability of the local authority to use the personal information for the purpose it was collected.[409]

Local authorities should use this provision in limited circumstances within programs, and the local authority should maintain documentation of when the provision has been used and the reasons for using it.[410]

IPC Findings

In Investigation Report F-2009-001, the Commissioner investigated a complaint involving the Saskatchewan Workers' Compensation Board (WCB). An individual had concerns about the way WCB collected, used and disclosed his personal information. As part of the investigation, the Commissioner considered WCB's collection of the complainant's personal information indirectly from the Sergeant-at-Arms with the Legislative Assembly Services. The Commissioner found that subsection 26(3) of *The Freedom of Information and Protection of Privacy Act* authorized the WCB to collect the complainant's personal information indirectly under this provision – equivalent provision to subsection 25(3) of LA FOIP.

[406] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 1221.
[407] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 250.
[408] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 375.
[409] Adapted from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 149. This definition is also consistent with the definition for "prejudice" found in various sections in Part III of FOIP – see *Guide to FOIP*, Chapter 4 – "Exemptions from the Right of Access".
[410] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 250.

Section 26: Standard of Accuracy

Standard of accuracy

26 A local authority shall ensure that personal information being used by the local authority for an administrative purpose is as accurate and complete as is reasonably possible.

Section 26 of LA FOIP requires that local authorities ensure that personal information being used for an administrative purpose is as accurate and complete as is reasonably possible. This requirement is intended to minimize the possibility that a decision affecting an individual will be made based on inaccurate, obsolete, or incomplete information.[411]

Section 26 incorporates a fundamental principle of "fair information practices" (see *10 Fair Information Principles, Accuracy* earlier in this Chapter), in that it requires that local authorities who use personal information to make decisions about an individual ensure the information is accurate and complete. The importance of this "data quality" principle cannot be overstated; its absence can lead to serious consequences.[412]

Administrative purpose means the use of personal information about an individual in a decision-making process that directly affects the individual. This includes all uses of personal information for confirming identity (i.e., authentication and verification purposes) and for determining eligibility of individuals for local authority programs.[413]

Accurate means careful, precise, lacking errors.[414]

Inaccurate information means wrong, incomplete, or misleading information or information that does not reflect the truth.[415]

---

[411] Drapeau, Professor Michel W., Racicot, Me Marc-Auréle, *Federal Access to Information and Privacy Legislation Annotated 2021,* (Toronto: Thomson Reuters 2020) at p. 6-84.
[412] SK OIPC Review Report F-2006-003 at [49]. Originates from AB IPC Order 98-002 at [86] and [87].
[413] Government of Canada, Treasury Board Secretariat, *Access to information and privacy, Policies, directives, standards and guidelines*. Available at Policy on Privacy Protection- Canada.ca.
[414] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 251. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-95. Available at Chapter (gov.mb.ca). Accessed December 13, 2022.
[415] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Complete means including every item or element, without omissions or deficiencies; not lacking in any element or particular. Information is complete when all the information necessary for the administrative purpose, and only the information necessary, is used.[416]

LA FOIP does not define the phrase "reasonably possible". However, the dictionary meanings of these words are as follows:

Reasonably possible:

> **Reasonable** means what a reasonable person would consider appropriate in the circumstances.[417] This standard acknowledges that reasonable "does not mean perfect".[418] It means fair, proper, moderate under the circumstances.[419]
>
> **Possible** means capable of existing, happening or being achieved.[420]

The extent to which personal information is accurate, complete and up to date will depend upon the use of the information, taking into account the interests of the individual.

Information shall be sufficiently accurate, complete, and up to date to minimize the possibility that inappropriate information may be used to make a decision about the individual.[421]

Generally, if a local authority collects personal information directly from an individual, the risk is lower that the information is inaccurate or incomplete. The risk increases when a local authority collects personal information indirectly. The burden of meeting the "reasonably

---

[416] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 251. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-95. Available at Chapter (gov.mb.ca). Accessed December 13, 2022.
[417] British Columbia's *Personal Information Protection Act*, SBC 2003, c 63 at section 2 and subsection 4(1). See also section 2 of Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5 and the joint resource by the Service Alberta and Alberta IPC titled, *A Guide for Businesses and Organizations on the Personal Information Protection Act* at p. 9.
[418] BC IPC Investigation Report F06-01 at [49].
[419] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p 1518. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-96. Available at Chapter (gov.mb.ca). Accessed December 13, 2022.
[420] See SK OIPC Review Report 082-2019, 083-2019 at [72] Originates from Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 1117.
[421] SK OIPC Investigation Reports F-2009-001 at [91] and LA-2013-001 at [35]. Originated from Saskatchewan Justice (now Ministry of Justice) resource, *An Overarching Personal Information Privacy Framework for Executive Government,* 2003 at p. 17.

possible" requirement is greater when the consequences of a decision are greater for the individual.[422]

When updating personal information, always consider the reason or purpose it was collected. It is not necessary to routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.[423]

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up to date, unless limits to the requirement for accuracy are clearly set out.[424]

Local authorities should have adequate procedures in place to properly verify the accuracy and completeness of any personal information crucial to an application, transaction, or action at the time the information is provided.[425]

It is a good business practice for programs that use large personal information systems for delivery of programs or services to have systematic processes for updating personal information that is used on a regular or continuous basis.[426]

Other methods of maintaining accuracy include:

- Periodically auditing files with accuracy and completeness being one of the criteria tested during the audit.
- Implementing procedures to update personal information that is used on a regular or continuous basis.
- Ensuring limited access to information for the purposes of making corrections or changes.

---

[422] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 251.
[423] SK OIPC Investigation Reports F-2009-001 at [91] and LA-2013-001 at [35]. Originated from Saskatchewan Justice (now Ministry of Justice) resource, *An Overarching Personal Information Privacy Framework for Executive Government,* 2003 at p. 17.
[424] SK OIPC Investigation Reports F-2009-001 at [91] and LA-2013-001 at [35]. Originated from Saskatchewan Justice (now Ministry of Justice) resource, *An Overarching Personal Information Privacy Framework for Executive Government,* 2003 at p. 17.
[425] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 251. Also quoted in SK OIPC Review Report F-2006-003 at [52].
[426] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 251. Also quoted in SK OIPC Review Report F-2006-003 at [52].

- Establishing cross referencing and verification checks within software of automated systems that identify anomalies in data. Privacy requirements should be integrated into normal information and systems operations for the program.[427]

Before using personal information to make a decision that affects an individual, the following questions may be helpful in assessing its accuracy and completeness:

- Was the personal information collected directly from the individual it is about.
- Was the accuracy of the personal information verified at the time it was collected.
- Is the proposed use of the personal information consistent with the purpose for which it was collected.
- What is the likelihood that the personal information is outdated. How old is the information. Is it likely that circumstances have changed since the information was collected.
- Are there systems in place to check the accuracy and completeness of the personal information – for example, periodic audits of files for accuracy, cross- referencing to other related files, systematic procedures for updating personal information, etc.?[428]

IPC Findings

In Investigation Report F-2009-001, the Commissioner investigated a complaint involving the Saskatchewan Workers' Compensation Board (WCB). An individual had concerns about the way WCB collected, used and disclosed his personal information. During the Commissioner's investigation, the Commissioner found evidence that raised whether the WCB met its duty to ensure accuracy in the personal information it uses for an administrative purpose and that such information be complete. The Commissioner found that WCB had appropriately developed a policy called *Safety and Security Policy* which included several checks and balances to ensure that decisions made under the policy would be evidence based and properly substantiated. However, the policy did not appear to have been followed in that case. Specially, the factual basis upon which WCB classified the complainant as a C4 and later a C5 risk was demonstrably incomplete. The Commissioner noted the high prejudice that

[427] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, pp. 251 to 252. Also quoted in SK OIPC Review Report F-2006-003 at [52]. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-96. Available at Chapter (gov.mb.ca). Accessed December 13, 2022.

[428] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at pp. 6-96 to 6-97. Available at Chapter (gov.mb.ca). Accessed December 13, 2022.

attaches to anyone who was classified as a security risk by the WCB and therefore it was incumbent on WCB to have a clear policy and procedure and to scrupulously follow it.

In Investigation Report F-2012-001, the Commissioner considered the over-collection of personal information by Saskatchewan Telecommunications (SaskTel). The Commissioner investigated SaskTel's collection of unique identifiers when customers call into SaskTel to access their account information for the purpose of identity verification. This included having to provide a date of birth, telephone number, social insurance number and health services number. The Commissioner found that SaskTel was not meeting its duty under the equivalent section 27 of *The Freedom of Information and Protection of Privacy Act* (FOIP) to collect accurate and complete information because SaskTel indicated that the information did not have to be accurate to verify identity. This appeared to serve the purpose of being a password rather than an accurate collection of personal information. As such, section 27 of FOIP was not met by SaskTel.

Section 27: Use of Personal Information

Use of personal information

27 No local authority shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:

(a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or

(b) for a purpose for which the information may be disclosed to the local authority pursuant to subsection 28(2).

Section 27 of LA FOIP provides that a local authority needs the consent of the individual to "use" their personal information unless one of the two enumerated circumstances exists.

Consent means voluntary agreement by a person in the possession and exercise of sufficient mental capacity to make an intelligent choice to do something proposed by another; it supposes a physical power to act, a moral power of acting and a serious, determined, and free use of these powers.[429]

[429] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Section 27 requires consent be given in "the prescribed manner". Subsection 2(i) of LA FOIP provides:

> **2** In this Act:
>
> …
>
> (h) **"prescribed"** means prescribed in the regulations;

Section 11 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* sets out the manner in which consent should be acquired:

> **11**(1) If consent is required by the Act for the collection, use or disclosure of personal information, the consent:
>
> (a) must relate to the purpose for which the information is required;
> (b) must be informed;
> (c) must be given voluntarily; and
> (d) must not be obtained through misrepresentation, fraud or coercion.
>
> (2) A consent to the collection, use or disclosure of personal information is informed if the individual who gives the consent is provided with the information that a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure of personal information.
>
> (3) A consent may be given that is effective for a limited period.
>
> (4) A consent may be express or implied unless otherwise provided.
>
> (5) An express consent need not be in writing.
>
> (6) A local authority, other than the local authority that obtained the consent, may act in accordance with an express consent in writing or a record of an express consent having been given without verifying that the consent meets the requirements of subsection (1) unless the local authority that intends to act has reason to believe that the consent does not meet those requirements.

Where reasonable, an individual's consent should be in writing. If consent is given verbally, the local authority should make a written record of the conversation and, where reasonable, send a letter to the individual confirming authorization.[430]

For more on consent and best practices, see *Consent* and *Best Practices for Consent Forms* earlier in this Chapter.

Section 27 of LA FOIP lists two circumstances under which a local authority is authorized to "use" personal information without the individual's consent:

1. Where the use is for the same purpose or a consistent purpose for which the personal information was collected.

2. For a purpose for which the personal information may be disclosed to the local authority.

Use indicates internal utilization of personal information by a local authority and includes the sharing of the personal information in such a way that it remains under the control of the local authority.[431]

"Use" should not be confused with "disclosure". Here is an easy way to decipher which it is:

- If the local authority shares the personal information internally amongst other divisions, programs, or employees, this is an internal "use" of the personal information not a "disclosure".

    - Sharing with contracted employees is also an internal "use" as they qualify as "employees of a local authority" pursuant to subsection 2(b.1) of LA FOIP. Contracted companies or agents providing services on behalf of the local authority are also captured as they are not considered separate from the local authority and are receiving and using the personal information "on behalf of" the local authority. Agreements or contracts should spell out privacy

[430] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Appendix 1 – Glossary of Terms* at p. 13. Available at *Resource Manual | FIPPA | Province of Manitoba (gov.mb.ca)* at Chapter 6., p. 6-56. Accessed December 5, 2022.
[431] First defined by SK OIPC in *2008-2009 Annual Report* at p. 76. First cited in Investigation Report F-2009-001 at [78].

responsibilities. See *"Use" Involving Contracted Third Parties* later in this Chapter.

- If the local authority shares the personal information outside of the organization, this is generally a "disclosure".
    - "Disclosure" includes sharing personal information with another local authority, as each is considered a separate "local authority" under LA FOIP.

Local authorities should still abide by the data minimization and need-to-know principles when using personal information. Only use the least amount of personal information necessary to achieve the purpose. Further, only share internally with those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

Subsection 27(a)

Use of personal information

27 No local authority shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:

(a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or

Subsection 27(a) of LA FOIP allows a local authority to use personal information for purposes consistent with the reason it was collected.

Use indicates internal utilization of personal information by a local authority and includes the sharing of the personal information in such a way that it remains under the control of the local authority.[432]

Purpose means the purpose for which personal information was obtained or compiled, the object to be attained or the thing intended to be done, e.g., the administration of a program,

[432] First defined by SK OIPC in *2008-2009 Annual Report* at p. 76. First cited in Investigation Report F-2009-001 at [78]. Originates from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 261.

the provision of a service or other activity.[433] The purpose of a collection means the reason(s) the personal information is needed and the use(s) that the local authority will make of the personal information.[434]

Original purpose is the specific reason for which the personal information was collected or created in the first place.[435]

> *Example:* a local authority collects certain employment history information about employees to administer benefit programs and that information can subsequently be used to determine the employee's eligibility for a certain program.

Consistent purpose is one that has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or for operating a legally authorized program of, the local authority that uses the personal information.[436]

A purpose is consistent and compatible where an individual might reasonably have expected the use of the personal information at the time of collection.[437]

Consistent use is a use of personal information that has a reasonable and direct connection to the specific reason for which it was collected or created in the first place. This means that the original use and the proposed use are so closely related that an individual would expect that the information would also be used for the second purpose (consistent purpose), even if the use is not spelled out.[438]

---

[433] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[434] SK OIPC Investigation Report F-2012-001 at [62]. Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 248.
[435] Office of the Privacy Commissioner of Canada, *Access to Information and Privacy Process and Compliance Manual for the OPC*, available at Access to Information and Privacy Process and Compliance Manual for the OPC - Office of the Privacy Commissioner of Canada. Accessed December 14, 2022.
[436] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 261.
[437] Ministry of Government and Consumer Services, Information, Privacy and Archives, *Freedom of* Ontario *Information and Protection of Privacy Manual* at p. 140. Available at https://files.ontario.ca/books/foi_privacy_manual_-_final-v02-2018-03-08-en-accessible.pdf. Accessed July 8, 2020.
[438] Office of the Privacy Commissioner of Canada, *Access to Information and Privacy Process and Compliance Manual for the OPC*, available at Access to Information and Privacy Process and Compliance Manual for the OPC - Office of the Privacy Commissioner of Canada. Accessed December 14, 2022.

Example: information in an employee's annual Performance Evaluation Report is originally collected to evaluate performance – it is not collected specifically for later use in staffing actions in which the employee may be involved. Still, the use of the information in a staffing context is wholly compatible with the reason for the original collection of the information. A logical link is made between the two uses, because the information collected in an appraisal reflects the strengths and weaknesses of the employee which may indicate whether that person is a good fit for the position to which they have applied.

Example of inconsistent or non-consistent use (improper): A community college collects personal information to survey community college students for their views on the college's course content in an effort to modify courses to meet changing needs of the student population. The college may use the information it collects from the students only to compile statistics or a report on the students' views. It may not subsequently use the information for a second, totally unrelated purpose (e.g., to lower the marks of those students who gave unfavourable comments on the course professors).[439]

Obtained means to acquire in any way; to get possession of; to procure; or to get a hold of by effort.[440]

Compiled means that the information was drawn from several sources or extracted, extrapolated, calculated or in some other way manipulated.[441] For example, a local authority creates or assigns an ID number for each client. This information becomes the personal information of the client, but the ID number was compiled by the local authority not collected from the client or indirectly from somewhere else.

The purpose for collection is described in the collection notification provided to the individual when the information is collected directly (see *Subsection 25(2)* earlier in this Chapter). When personal information is not collected directly, or when it is compiled from several sources, the purpose should be stated in the written policy or procedure dealing with the program.[442]

---

[439] British Columbia Government Services, *FOIPPA Policy Definitions*, available at Section 32 - Use of Personal Information - Province of British Columbia (gov.bc.ca). Accessed December 14, 2022.
[440] Originated from Campbell Black, Henry, 1990. *Black's Law Dictionary, 6th Edition.* St. Paul, Minn.: West Group. Adopted by AB IPC in Order 2000-021 at [26]. Adopted in SK OIPC Review Report F-2006-001 at [58] and [59]. Also, found in SK OIPC Review Report F-2006-002 at [39].
[441] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[442] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 260.

In most cases, the local authority using the information, will be the local authority that collected it. However, if the personal information has been collected for the purposes of delivering a common or integrated service, the local authority using the information may not be the local authority that originally collected it.[443] See section 10.1 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* for more on common or integrated services.

Local authorities should still abide by the data minimization and need-to-know principles when using personal information. Only use the least amount of personal information necessary to achieve the purpose. Further, only share internally with those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 090-2017, the Commissioner investigated a privacy complaint involving the City of Saskatoon. The complainant alleged their privacy was breached when the City used a video recording from surveillance cameras to investigate whether the complainant, a bus driver, conducted himself appropriately during a shift. The Commissioner found that the City had authority under subsection 27(a) of LA FOIP to use the complainant's personal information for the purpose of its investigation.

In Investigation Report 234-2020, the Commissioner investigated a privacy complaint involving Chinook School Division No. 211. The complainant alleged that Chinook School Division was forwarding emails that she had been sending to the school division. The individuals receiving the emails were not on the consent form she had signed. The Commissioner found that subsection 27(a) of LA FOIP authorized the use of the Complainant's daughter's personal information in some instances, but not in all. The Commissioner made a number of recommendations including that Chinook School Division ensure its privacy policies and procedures address the need-to-know principle along with other recommendations.

In Investigation Report 021-2018, the Commissioner investigated a privacy complaint involving the City of Regina. The complainant alleged that the City breached their privacy by collecting, using, and disclosing the individual's personal information contained in text messages. The Commissioner found that the City collected and used the text messages for the purpose of a workplace investigation which fell under the activity of managing

[443] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 294.

employees. The Commissioner found that the City had authority to collect the personal information but also to use it for this purpose pursuant to subsection 27(a) of LA FOIP because the use was consistent with the original purpose for which the text messages were collected.

Subsection 27(b)

Use of personal information

27 No local authority shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:

...

(b) for a purpose for which the information may be disclosed to the local authority pursuant to subsection 28(2).

Subsection 27(b) of LA FOIP permits a local authority to use personal information that has been disclosed to it by another local authority under subsection 28(2) of LA FOIP.

Where local authority "A" has received personal information from local authority "B" under subsection 28(2) of LA FOIP, local authority "A" may use that information for the purpose for which it was disclosed by local authority "B".[444]

Without this provision, a local authority would be unable to use personal information which other local authorities are authorized to disclose to them.[445] In appropriate circumstances, subsection 27(b) of LA FOIP can reduce the number of times an individual must provide the same personal information to local authorities and can reduce the cost of gathering personal information required by more than one local authority.[446]

---

[444] British Columbia Government Services, *FOIPPA Policy Definitions*, available at Section 32 - Use of Personal Information - Province of British Columbia (gov.bc.ca). Accessed December 14, 2022. See also Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 263, and Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-139. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.

[445] British Columbia Government Services, *FOIPPA Policy Definitions*, available at Section 32 - Use of Personal Information - Province of British Columbia (gov.bc.ca). Accessed December 14, 2022. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-139. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.

[446] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-139. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.

A local authority can disclose personal information provided there is authority to do so under subsection 28(2) of LA FOIP. Subsection 28(2) of LA FOIP provides numerous circumstances under which a local authority may disclose personal information without consent of the individual for which it pertains. See *Subsection 28(2)(a)* through *28(2)(s)* later in this Chapter.

However, the local authority that is receiving the personal information, should ensure that it has authority to collect the personal information in the first place under section 24 of LA FOIP (i.e., before relying on subsection 27(b) of LA FOIP to "use" it). If the local authority finds authority under section 24 to collect the personal information, it should also consider subsection 25(3) of LA FOIP for authority to collect the personal information "indirectly".

Local authorities should still abide by the data minimization and need-to-know principles when using personal information. Only use the least amount of personal information necessary to achieve the purpose. Further, only share internally with those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

Example:

One local authority issues a subpoena to a second local authority, as part of a court case it is preparing. The second local authority is authorized to disclose personal information to the first local authority under subsection 28(2)(b)(i) of LA FOIP in response to the subpoena. Subsection 27(b) of LA FOIP permits the first local authority to "use" that personal information for its court case.

Example:

A local authority has a client who has just died. It wishes to contact the next of kin of the deceased to inform them of the death but does not have the relative's address. A second local authority does have the address and, on the request of the first local authority, may disclose it in accordance with subsection 28(2)(m) of LA FOIP. The first local authority may in turn "use" the personal information (address) solely in order to contact the relative and may not "use" it for any other purpose.

Interpretation Note

Many Reports by the Commissioner have been issued over the years for subsection 27(b) of LA FOIP and the equivalent subsection 28(b) of *The Freedom of Information and Protection of Privacy Act* (FOIP). However, those reports reflect a former interpretation of this provision.

The former interpretation was that a local authority could "use" personal information for a purpose it could also "disclose" that personal information. This former interpretation was consistent with the Office of the Alberta Information and Privacy Commissioner's (AB IPC) interpretation of a similar provision in Alberta's FOIP Act. However, AB IPC shifted its interpretation.

At the present time, British Columbia, Alberta, and Manitoba all have provisions in their FOIP Acts that are similarly worded to Saskatchewan's 27(b) of LA FOIP and all three have interpretations consistent with each other. The guidance reflected in this Chapter is consistent with the interpretations of these other provinces.

As of the issuing of this Chapter, the interpretation for subsection 27(b) of LA FOIP will be shifting to adopt this new interpretation reflected in this Chapter and would be consistent with British Columbia, Alberta and Manitoba.

Reports issued prior to this Chapter would not reflect this new interpretation but rather the old one.

"Use" Involving Contracted Third Parties

In the privacy world, when records are provided to a contractor and yet remain under the control of a local authority this constitutes a "use" and not a "disclosure". In other words, there is no disclosure if the local authority retains control over the records.

"*Transfer*" is a use by the local authority. It is not to be confused with a disclosure. When a local authority transfers personal information for processing, it can only be used for the purposes for which the information was originally collected.

> *Example:* transferring of personal information for the purpose of processing payments to customers.
>
> *Example:* an internet service provider may transfer personal information to a third party to ensure that technical support is available on a 24/7 basis.

Increasingly, local authorities outsource processes to third parties. In many cases, this involves the transfer of personal information. A contractor works "on behalf of" the local authority like what would be done by an employee of the local authority.

Therefore, since the contractor is working on behalf of the local authority, the transfer of records to the contractor is a "use," not a "disclosure."

Through a contract, the contractor uses the information to fulfill the local authority's purpose for collecting the personal information in the first place.[447]

Local authorities are responsible for the actions of its contractors and agents when it comes to the protection of personal information it shares with its contractors and agents. Therefore, a strong written contract or agreement should be in place that spells out the privacy obligations the contractor or agent must abide by (which are the same obligations on the local authority).

Subcontracting by Outsourcers

Subcontracting by outsourcers is a concern that local authorities should take into consideration. A local authority having a contract with an outsource partner has a direct, legal relationship with that partner. It is aware of the contractual rights and remedies and can exercise them directly vis-à-vis its contracted partner.

Furthermore, a local authority can choose who to contract with, exercising whatever due diligence it deems necessary in making the selection. This is not necessarily the case with sub-contracted outsourcers.

The principle contracted outsourcer may choose its subcontractors based on entirely different criteria than would the local authority. A breach of the subcontract may only be actionable by the contractor; the local authority may have no ability to deal with the subcontractor except through the principal contractor.[448]

[447] SK OIPC Investigation Report F-2013-001 at [76] to [78].
[448] SK OIPC Investigation Report F-2013-001 at [114]. Originates from AB IPC resource, *Public-sector Outsourcing and Risks to Privacy*, February 2006 at p. 28.

Section 28: Disclosure of Personal Information

Disclosure of personal information

28(1) No local authority shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 29.

(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

(a) for the purpose for which the information was obtained or compiled by the local authority or for a use that is consistent with that purpose;

(b) for the purpose of complying with:

(i) a subpoena or warrant issued or order made by a court, person or body that has the authority to compel the production of information; or

(ii) rules of court that relate to the production of information;

(c) to the Attorney General for Saskatchewan or to his or her agent or legal counsel for use in providing legal services to the Government of Saskatchewan or a government institution;

(d) to legal counsel for a local authority for use in providing legal services to the local authority;

(e) for the purpose of enforcing any legal right that the local authority has against any individual;

(f) for the purpose of locating an individual in order to collect a debt owing to the local authority by that individual or make a payment owing to that individual by the local authority;

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met;

(h) pursuant to an agreement or arrangement between the local authority and:

(i) the Government of Canada or its agencies, Crown corporations or other institutions;

(ii) the Government of Saskatchewan or a government institution;

(iii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

Office of the Saskatchewan Information and Privacy Commissioner. Guide to LA FOIP, Chapter 6, *Protection of Privacy*. Updated 27 February 2023.

(iv) the government of a foreign jurisdiction or its institutions;

(v) an international organization of states or its institutions; or

(vi) another local authority;

for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(h.1) for any purpose related to the detection, investigation or prevention of an act or omission that might constitute a terrorist activity as defined in the *Criminal Code*, to:

(i) a government institution;

(ii) the Government of Canada or its agencies, Crown corporations or other institutions;

(iii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iv) the government of a foreign jurisdiction or its institutions;

(v) an international organization of states or its institutions; or

(vi) another local authority;

(i) for the purpose of complying with:

(i) an Act or a regulation;

(ii) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada; or

(iii) a treaty, agreement or arrangement made pursuant to an Act or an Act of the Parliament of Canada;

(j) where disclosure is by a law enforcement agency:

(i) to a law enforcement agency in Canada; or

(ii) to a law enforcement agency in a foreign country;

pursuant to an arrangement, a written agreement or treaty or to legislative authority;

(k) to any person or body for research or statistical purposes if the head:

(i) is satisfied that the purpose for which the information is to be disclosed is not contrary to the public interest and cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates; and

(ii) obtains from the person or body a written agreement not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;

(l) where necessary to protect the mental or physical health or safety of any individual;

(m) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;

(n) for any purpose where, in the opinion of the head:

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or

(ii) disclosure would clearly benefit the individual to whom the information relates;

(o) to the Government of Canada or the Government of Saskatchewan to facilitate the auditing of shared cost programs;

(p) if the information is publicly available, including information that is prescribed as publicly available;

(q) to the commissioner;

(r) for any purpose in accordance with any Act or regulation that authorizes disclosure; or

(s) as prescribed in the regulations.

Section 28 of LA FOIP prohibits the disclosure of personal information unless the individual about whom the information pertains consents to its disclosure or if disclosure without consent is authorized by one of the enumerated subsections of 28(2) or section 29 of LA FOIP.

Disclosure is sharing of personal information with a separate entity, not a division or branch of the local authority in possession or control of that information.[449]

Exceptions to disclosure with consent are outlined at subsection 28(2) and section 29 of LA FOIP. In addition, sections 10, 10.1 and 10.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations*. If one of these exceptions applies, the local authority may disclose without the consent of the individual.

Section 28 of LA FOIP only applies to personal information as defined by section 23 of LA FOIP. For the definition and interpretation of what qualifies as "personal information" see *Section 23* earlier in this Chapter.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know

[449] First defined by SK OIPC in *2008-2009 Annual Report* at p. 74.

the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

Subsection 28(1)

Disclosure of personal information

28(1) No local authority shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 29.

Subsection 28(1) of LA FOIP requires a local authority to have consent of the individual prior to disclosing that person's personal information.

Disclosure is sharing of personal information with a separate entity, not a division or branch of the local authority in possession or control of that information.[450]

Consent means voluntary agreement by a person in the possession and exercise of sufficient mental capacity to make an intelligent choice to do something proposed by another; it supposes a physical power to act, a moral power of acting and a serious, determined, and free use of these powers.[451]

Subsection 28(1) of LA FOIP requires consent be given in "the prescribed manner". Subsection 2(i) of LA FOIP provides:

> **2** In this Act:
>
> ...
>
> (i) **"prescribed"** means prescribed in the regulations;

Section 11 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* sets out the manner in which consent should be acquired:

> **11**(1) If consent is required by the Act for the collection, use or disclosure of personal information, the consent:

---

[450] First defined by SK OIPC in *2008-2009 Annual Report* at p. 74.
[451] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

(a) must relate to the purpose for which the information is required;
(b) must be informed;
(c) must be given voluntarily; and
(d) must not be obtained through misrepresentation, fraud or coercion.

(2) A consent to the collection, use or disclosure of personal information is informed if the individual who gives the consent is provided with the information that a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure of personal information.

(3) A consent may be given that is effective for a limited period.

(4) A consent may be express or implied unless otherwise provided.

(5) An express consent need not be in writing.

(6) A local authority, other than the local authority that obtained the consent, may act in accordance with an express consent in writing or a record of an express consent having been given without verifying that the consent meets the requirements of subsection (1) unless the local authority that intends to act has reason to believe that the consent does not meet those requirements.

Where reasonable, an individual's consent should be in writing. If consent is given verbally, the local authority should make a written record of the conversation and, where reasonable, send a letter to the individual confirming authorization.[452]

For more on consent and best practices, see *Consent* and *Best Practices for Consent Forms* earlier in this Chapter.

Without consent, personal information cannot be released unless one of the provisions under subsection 28(2) or section 29 of LA FOIP applies. In addition, sections 10, 10.1 and 10.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations*. See the subsections below for detailed guidance on subsection 28(2) and section 29 of LA FOIP.

[452] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Appendix 1 – Glossary of Terms* at p. 13. Available at *Resource Manual | FIPPA | Province of Manitoba (gov.mb.ca)* at Chapter 6., p. 6-56. Accessed December 5, 2022.

Subsection 28(2)(a)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

(a) for the purpose for which the information was obtained or compiled by the local authority or for a use that is consistent with that purpose;

Subsection 28(2) of LA FOIP provides several circumstances where a local authority can disclose personal information without the consent of the individual whose personal information is involved. There are additional circumstances enumerated in the LA FOIP Regulations.

Subsection 28(2)(a) of LA FOIP provides that a local authority may disclose an individual's personal information for the same purpose for which it was originally obtained or compiled or for a "use" that is consistent with that purpose.

Purpose means the purpose for which personal information was obtained or compiled, the object to be attained or the thing intended to be done, e.g., the administration of a program, the provision of a service or other activity.[453] The purpose of a collection means the reason(s) the personal information is needed and the use(s) that the local authority will make of the personal information.[454]

Use indicates internal utilization of personal information by a local authority and includes the sharing of the personal information in such a way that it remains under the control of the local authority.[455]

---

[453] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[454] SK OIPC Investigation Report F-2012-001 at [62]. Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 248.
[455] First defined by SK OIPC in *2008-2009 Annual Report* at p. 76. First cited in Investigation Report F-2009-001 at [78]. Originates from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p 261.

Consistent purpose is one that has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or for operating a legally authorized program of, the local authority that uses the personal information.[456]

A purpose is consistent and compatible where an individual might reasonably have expected the disclosure of the personal information at the time of collection. For example, disclosing the name and address of an individual to a courier company for the purpose of delivering a package would be considered a consistent purpose where the individual had requested new vehicle licence plates.[457]

Obtained means to acquire in any way; to get possession of; to procure; or to get a hold of by effort.[458]

Compiled means that the information was drawn from several sources or extracted, extrapolated, calculated or in some other way manipulated.[459]

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 059-2018, the Commissioner investigated a complaint involving the Town of Fort Qu'Appelle (Fort Qu'Appelle). The complaint alleged that Fort Qu'Appelle disclosed the individual's personal information contained in a petition. Upon investigation, the Commissioner found that Fort Qu'Appelle had authority to disclose the personal

---

[456] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 261.
[457] Ontario Ministry of Government and Consumer Services, Information, Privacy and Archives, *Freedom of Information and Protection of Privacy Manual* at p. 140. Available at https://files.ontario.ca/books/foi_privacy_manual_-_final-v02-2018-03-08-en-accessible.pdf. Accessed July 8, 2020.
[458] Originated from Campbell Black, Henry, 1990. *Black's Law Dictionary, 6th Edition.* St. Paul, Minn.: West Group. Adopted by AB IPC in Order 2000-021 at [26]. Adopted in SK OIPC Review Report F-2006-001 at [58] and [59]. Also, found in SK OIPC Review Report F-2006-002 at [39]. Definition is also found in SK OIPC resource, *IPC Guide to FOIP,* Chapter 4.
[459] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

information in the petition pursuant to subsection 28(2)(a) of LA FOIP. In coming to this finding, the Commissioner found that petitions are not intended to be kept secret. The names of individuals signing petitions are not normally supplied in confidence.

In Investigation Report 062-2016, the Commissioner investigated a complaint involving Keewatin Yatthe Regional Health Authority (Keewatin). The complaint alleged that Keewatin inappropriately used the individual's personal information (employee conduct) when it disclosed the personal information to the Saskatchewan Union of Nurses (SUN). The Commissioner found that SUN was the union that would represent the individual, as an Occupational Health and Safety investigation had occurred, it was reasonable for Keewatin to notify SUN that one of their members had faced an investigation relating to professional misconduct and harassment. The Commissioner found the disclosure was authorized by subsection 28(2)(a) of LA FOIP.

Subsection 28(2)(b)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(b) for the purpose of complying with:

(i) a subpoena or warrant issued or order made by a court, person or body that has the authority to compel the production of information; or

(ii) rules of court that relate to the production of information;

Subsection 28(2)(b) of LA FOIP permits a local authority to disclose personal information without consent for the purpose of complying with a subpoena, warrant or order that compels the production of information or to comply with rules of court that relate to the production of information.

Subsection 28(2)(b)(i)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

…

(b) for the purpose of complying with:

(i) a subpoena or warrant issued or order made by a court, person or body that has the authority to compel the production of information; or

Subsection 28(2)(b)(i) of LA FOIP provides that a local authority can disclose personal information without consent if it is for the purpose of complying with a subpoena or warrant or order.

To **comply** with a subpoena, warrant or order means to act in accordance with or fulfill the requirements of the subpoena, warrant or order.[460]

A **subpoena** (can also be called a "summons to witness") is a command issued by a party in litigation requiring the attendance of someone as a witness at a court proceeding or hearing. It will specify a certain place and time when testimony on a certain matter will be required and may also order a person to meet the requirements of a court to disclose information.[461] A subpoena may also require the person to bring records, documents, files or other specified information to the court or the hearing.[462]

Time is usually of the essence in dealing with a subpoena, as it is often served with very little notice. Local authorities cannot ignore subpoenas since they would risk being cited for contempt of court and, at a minimum, fined.[463]

A **warrant** is a judicial authorization to collect information – in this context, personal information.[464] It is an order of a judicial authority authorizing an officer named or described

[460] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-184. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[461] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 273.
[462] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-184. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[463] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 273.
[464] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 273.

in the warrant to arrest a person, seize something (such as records), search something (such as a computer or premises) or execute or carry out some judicial sentence.[465]

An **order** is an authoritative command, direction, or instruction to produce something – again in this context, personal information.[466] It is a direction of a court, judge, tribunal or official that commands a party to do or not to do something; a judgement, decree, direction or decision that is authorized or required to be made under a statute or regulation.[467]

The subpoena, warrant or order must be made by a court, person or body that had authority to compel production of personal information. This authority is generally found under legislation of Saskatchewan or Canada.

Official, bodies or tribunals who are not judges or courts only have authority to issue orders compelling attendance at a hearing or compelling production of documents or other information if that power is given to them by a statute or regulation. Examples of officials, bodies or tribunals who have been given such authority include, but is not limited to:

- The Saskatchewan Labour Relations Board (via s. 2-83(3)(b) and (c) of *The Saskatchewan Employment Act*).
- The Saskatchewan Workers' Compensation Board (via s. 122(2)(b), 128(2) of *The Workers' Compensation Act)*.
- The Executive Director of the Financial and Consumer Affairs Authority (via s. 14.1 of *The Securities Act, 1988)*.
- A Commission of Inquiry established under *The Public Inquiries Act, 2013* (via s. 11 of that Act*)*.

Compel means to cause or bring about by force, threats, or overwhelming pressure.[468]

Although subsection 28(2)(b)(i) of LA FOIP enables, but does not require disclosure (i.e., by use of the word "may" and not "shall" disclose), local authorities normally comply with subpoenas, warrants and orders because they have the force of law. However, a local

---

[465] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-184. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[466] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 274.
[467] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-185. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[468] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 353.

authority should not automatically assume that subpoena, warrant, or order is valid in Saskatchewan.[469]

A local authority should consult with legal counsel immediately upon receipt of a subpoena, warrant or order to determine:

- Whether the document is properly authorized and drafted.
- Whether the document has been properly served.
- Whether the information required to be produced is legally compellable or whether there are some legal grounds for opposing the subpoena, warrant or order.
- What information must be provided to comply with the subpoena, warrant or order.[470]

Local authorities should keep subsections 4(c) and (d) of LA FOIP in mind when dealing with subsection 28(2)(b)(i) of LA FOIP.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Subsection 28(2)(b)(ii)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

…

[469] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 274.
[470] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at pp. 6-185 to 6-186. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.

(b) for the purpose of complying with:

...

(ii) rules of court that relate to the production of information;

Subsection 28(2)(b)(ii) of LA FOIP provides that a local authority can disclose personal information without consent if it is for the purpose of complying with rules of court that relate to the production of information.

To **comply** with rules of court means to act in accordance with or fulfill the requirements of the rules of court.[471]

Rules of court are the rules of procedures that govern all proceedings before the courts, each has its own rules of procedure.[472]

The rules of court govern the practices and procedures to be followed in matters that are brought before the Court. Compliance with the Rules is mandatory, and it is the responsibility of lawyers or persons who represent themselves in court proceedings to know and comply with the rules that may apply to their proceeding. Failure to comply can result in unnecessary delay and expense. It could also result in a significant disadvantage or loss in a person's ability to pursue a claim, appeal or defence.[473]

Examples of rules of court that relate to the production of information include:

- The Court of King's Bench Rules respecting discovery of documents in a civil court proceeding.
- The common law rules developed by the criminal courts respecting Crown disclosure in criminal cases.[474]

Local authorities should keep subsections 4(c) and (d) of LA FOIP in mind when dealing with subsection 28(2)(b)(ii) of LA FOIP.

---

[471] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-184. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[472] Courts of Saskatchewan, *Rules & Practice Directives,* available at RULES & PRACTICE DIRECTIVES | Saskatchewan Courts (sasklawcourts.ca). Accessed December 14, 2022.
[473] Courts of Saskatchewan, *Rules & Practice Directives,* available at RULES & PRACTICE DIRECTIVES | Saskatchewan Courts (sasklawcourts.ca). Accessed December 14, 2022.
[474] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-185. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Subsection 28(2)(c)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed:

...

(c) to the Attorney General for Saskatchewan or to his or her agent or legal counsel for use in providing legal services to the Government of Saskatchewan or a government institution;

Subsection 28(2)(c) of LA FOIP provides that a local authority can disclose personal information without consent to the Attorney General for Saskatchewan or his or her agent or legal counsel for use in providing legal services to the Government of Saskatchewan or a government institution.

Attorney General, in this context, is the chief law officer of Saskatchewan responsible for advising the government on legal matters and representing it in litigation.[475]

An **agent** of the Attorney General for Saskatchewan can include public prosecutions at the Ministry of Justice.[476]

[475] Modified from Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 154.
[476] SK OIPC Review Report F-2012-006 at [111].

Legal service includes any law related service performed by a person engaged by a local authority and who is licensed to practice law.[477] For purposes of this provision, the legal services must be provided to the Government of Saskatchewan or a government institution by the Attorney General for Saskatchewan or by his or her agent or legal counsel.

The Ministry of Justice can act as legal advisors for all departments of government.[478] Crown Counsel and Crown Prosecutors employed by the Ministry of Justice would fit within this provision.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Subsection 28(2)(d)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(d) to legal counsel for a local authority for use in providing legal services to the local authority;

Subsection 28(2)(d) of LA FOIP permits a local authority to disclose personal information to its legal counsel for use in providing legal services to the local authority.

[477] Definition originated from AB IPC Order 96-017 at [37]. Adopted in SK OIPC Review Report F-2012-003 at [96]. Adjusted to include "engaged by a local authority" in Review Report 171-2019 at [119].
[478] SK OIPC Review Report F-2005-002 at [26]. For this interpretation, the Commissioner, relied on *The Law of Evidence in Canada*.

Legal service includes any law-related service performed by a person engaged by a local authority and who is licensed to practice law.[479] For purposes of this provision, the legal services must be provided to the local authority by legal counsel. This can include a private bar legal counsel retained to act on behalf of the local authority.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 002-2018, the Commissioner investigated an alleged breach of privacy involving Saskatchewan Polytechnic (SaskPolytech). The complaint alleged SaskPolytech's legal counsel disclosed the complainant's personal information at an arbitration hearing. The Commissioner found that SaskPolytech had authority to disclose the Complainant's personal information at the arbitration hearing pursuant to subsection 28(2)(d) of LA FOIP.

Subsection 28(2)(e)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(e) for the purpose of enforcing any legal right that the local authority has against any individual;

Subsection 28(2)(e) of LA FOIP provides that a local authority can disclose personal information without consent for the purpose of enforcing any legal right that the local authority has against any individual.

[479] Definition originated from AB IPC Order 96-017 at [37]. Adopted in SK OIPC Review Report F-2012-003 at [96]. Adjusted to include "engaged by a local authority" in Review Report 171-2019 at [119]. It has been adapted to read "engaged by a local authority" for purposes of s. 28(2)(d) of LA FOIP.

The following three-part test can be applied:[480]

1. Does the local authority have a legal right

A **legal right** is a right based on a statute or regulation or on common law (that is, judge-made law).[481]

2. Is the legal right against an individual

Individual means natural persons (human beings).[482] Use of the word *individual* in this provision makes it clear that the enforcement of the legal right must be against only natural persons or human beings.[483]

3. Was disclosure made for the purpose of enforcing that legal right

Enforcement in this context means the act or process of compelling compliance with a legal right that the local authority has.[484]

Disclosure for purposes of this provision may be:

- To legal counsel.
- To any person authorized to enforce the legal right of the local authority.[485]

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know

---

[480] Three part test first introduced in SK OIPC Investigation Report 068-2020 at [33].
[481] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-189. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[482] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at pp. 924, 1238 and 1378.
[483] ON IPC Order 16 at p. 19. See also Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 2, Scope of FIPPA – Who and What Falls under FIPPA* at p. 44. Available at https://www.gov.mb.ca/fippa/public_bodies/resource_manual/pdfs/chap_2.pdf. Accessed on April 24, 2020.
[484] Adapted from Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 645.
[485] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-190. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.

the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 068-2020, the Commissioner investigated an alleged breach of privacy involving the Town of Qu'Appelle (Town). The complaint alleged that the Town breached the individual's privacy by disclosing a copy of a "Residential Contract of Purchase and Sale" to the Appeals Assessment Committee. The Town asserted that subsection 28(2)(e) of LA FOIP provided authority to disclose the sales agreement. The Commissioner found that the Town had authority to disclose the complainant's personal information pursuant to subsection 28(2)(e) of LA FOIP.

Subsection 28(2)(f)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

…

(f) for the purpose of locating an individual in order to collect a debt owing to the local authority by that individual or make a payment owing to that individual by the local authority;

Subsection 28(2)(f) of LA FOIP provides that a local authority can disclose personal information without consent for the purpose of locating an individual to collect a debt owed to the local authority or for the local authority to make a payment owed to the individual.

Sometimes, local authorities face the problem of not being able to locate an individual that owes money to the local authority, or the local authority owes the individual money.

The following two-part test can be applied:

1. Is the disclosure of personal information for the purpose of locating the individual?

To rely on this provision, the local authority must be disclosing the individual's personal information for the purpose of locating the individual to collect a debt from the individual or make a payment to the individual.

If the local authority is disclosing personal information but already knows where the individual is located, the provision cannot be relied upon.

Locate means to discover the exact place or position.[486] In this context, it means the act of locating an individual. "Location" means a particular place or position.[487]

2. Is locating the individual for the purpose of collecting a debt owed to the local authority or for the local authority to make a payment owed to the individual?

A **debt** is something that is owed, usually money, where the individual has an obligation to pay, and the creditor has the right to receive and enforce payment.[488] A debt is a specified amount of money due to the local authority.

A **payment** is a sum of money which a local authority owes to an individual.[489]

This provision does not permit disclosure of personal information by a local authority for the purpose of determining whether a debt or payment is owed. This determination must already be made.[490]

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information for this purpose. Only disclose the least amount of personal information necessary to achieve the purpose of locating the individual. It is generally not necessary to disclose the reason for the debt or payment (e.g., the penalty or offence leading to the debt owed). Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

---

[486] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 833.
[487] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.*, (Oxford University Press) at p. 833.
[488] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 277.
[489] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[490] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7, p. 278.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Subsection 28(2)(g)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met;

Subsection 28(2)(g) of LA FOIP permits a local authority to disclose personal information without consent to a "prescribed" law enforcement agency or "prescribed" investigative body where the enumerated circumstances exist at subsections 28(2)(g)(i) through (iii) of LA FOIP.

Section 9 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* (LA FOIP Regulations) defines the bodies that are considered law enforcement agencies and investigative bodies for purposes of subsection 28(2)(g) of LA FOIP. The list is extensive and includes subsections 9(a) through (aa) of the LA FOIP Regulations.

The purpose of this provision is to assist law enforcement or investigative bodies.

Subsection 28(2)(g) of LA FOIP requires that the law enforcement agency or investigative body be "prescribed". Subsection 2(i) of LA FOIP provides:

2 In this Act:

...

(i) **"prescribed"** means prescribed in the regulations;

Local authorities should refer to section 9 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* before disclosing to ensure the body being disclosed to qualifies as a "law enforcement agency" or "investigative body".

For subsection 28(2)(g) of LA FOIP to apply, the following circumstances must be met:

1. The disclosure must be made to a law enforcement agency or an investigative body that is prescribed in section 9 of *The Local Authority Freedom of Information and Protection of Privacy Regulations.*

2. The disclosure must be for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation.

3. The information must have been requested by the law enforcement agency or investigative body.

4. The disclosure must meet any requirements that are prescribed in *The Local Authority Freedom of Information and Protection of Privacy Regulations.*[491]

A **lawful investigation** is an investigation that is authorized or required and permitted by law.[492]

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 275-2017, the Commissioner investigated a complaint involving Saskatchewan Power Corporation (SaskPower). The complaint alleged that SaskPower disclosed the complainant's personal information to the Regina Police Service. SaskPower asserted it had authority to disclose the complainant's personal information without consent pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP) *(*subsection 29(2)(g)). The Commissioner found that the Regina Police Service (RPS)

[491] SK OIPC Investigation Report 275-2017 at [20].
[492] First defined in SK OIPC Review Report 93/021 at p. 6. Adopted in SK OIPC Review Report F-2004-006 at [26] and F-2014-001 at [160].

qualified as a "law enforcement agency" for purposes of subsection 29(2)(g) of FOIP. Further, that the disclosure was made for the purposes of an RPS investigation of a bomb threat which qualified as a "lawful investigation". Further, RPS requested the material from SaskPower. Finally, there were no additional requirements listed in *The Freedom of Information and Protection of Privacy Regulations*. Therefore, the Commissioner found that SaskPower had authority to disclose the complainant's personal information to the RPS pursuant to subsection 29(2)(g) of FOIP.

Subsection 28(2)(h)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(h) pursuant to an agreement or arrangement between the local authority and:

(i) the Government of Canada or its agencies, Crown corporations or other institutions;

(ii) the Government of Saskatchewan or a government institution;

(iii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iv) the government of a foreign jurisdiction or its institutions;

(v) an international organization of states or its institutions; or

(vi) another local authority;

for the purpose of administering or enforcing any law or carrying out a lawful investigation;

Subsection 28(2)(h) of LA FOIP permits a local authority to disclose personal information about an individual without consent for the purpose of administering or enforcing any law or carrying out a lawful investigation where there is an agreement or arrangement between the local authority and any of the enumerated parties listed at subsections 28(2)(h)(i) through (vi) of LA FOIP.

The enumerated parties listed include:

(i) The Government of Canada or its agencies, Crown corporations or other institutions.

For subsection 28(2)(h)(i) of LA FOIP to apply, the agencies in question must qualify as either "*Government of Canada or its agencies, Crown corporations or other institutions*". Because of the possessive pronoun in this clause, "agencies" and "other institutions" should be understood as federal agencies and federal institutions. For "other institutions", it should be either federal government institutions as defined by the federal *Access to Information Act* or institutions controlled by the federal government.[493]

For some assistance, Schedule 1 (Section 3) of the federal *Access to Information Act* provides a list of federal government institutions.

Government of Canada means the Crown in right of Canada.[494]

(ii) The Government of Saskatchewan or a government institution.

For subsection 28(2)(h)(ii) of LA FOIP to apply, the agencies in question must qualify as either the *"Government of Saskatchewan"* or a *"government institution"*.

Government of Saskatchewan has a broader meaning than "government institution". Government of Saskatchewan means the Crown in right of Saskatchewan.[495]

Government institution means a "government institution" as defined at subsection 2(1)(d) of *The Freedom of Information and Protection of Privacy Act*. It also includes boards, commissions, Crown corporations and other bodies prescribed in the Appendix, Part I of *The Freedom of Information and Protection of Privacy Regulations*.

(iii) The government of another province or territory of Canada, or its agencies, Crown corporations or other institutions.

For subsection 28(2)(h)(iii) of LA FOIP to apply, the agencies in question must qualify as a "g*overnment of another province or territory of Canada, or its agencies,*

[493] SK OIPC Review Report F-2006-002 at [23] and [32].
[494] *The Legislation Act*, SS 2019, c L-10.2 at s. 2-29.
[495] *The Legislation Act*, SS 2019, c L-10.2 at s. 2-29.

Crown corporations or other institutions". Because of the possessive pronoun in this clause, "agencies" and "other institutions" should be understood as provincial or territorial agencies and institutions. For "other institutions", it should be provincial or territorial government institutions as defined by those provinces and territories.[496]

(iv) The government of a foreign jurisdiction or its institutions.

For subsection 28(2)(h)(iv) of LA FOIP to apply, the agency in question must qualify as a "*government of a foreign jurisdiction or its institutions"*. A **foreign jurisdiction** refers to a government or its institutions of any foreign nation or state outside of Canada.[497]

(v) An international organization of states or its institutions.

For subsection 28(2)(h)(v) of LA FOIP to apply, the agency in question must qualify as a "*international organization of states or its institutions"*. An **international organization of states** refers to any organization with members representing and acting under the authority of the governments of two or more states. Examples include the United Nations and the International Monetary Fund.[498]

(vi) Another local authority.

For subsection 28(2)(h)(vi) of LA FOIP to apply, the agency in question must qualify as a "*local authority*". Subsection 2(f) *The Local Authority Freedom of Information and Protection of Privacy Act* defines which bodies qualify as local authorities.

Agreement means a mutual understanding between two or more parties as to a course of action[499]; a contract between two or more parties creating obligations that are enforceable or otherwise recognizable at law.[500] In this case, the agreement would generally be in writing. An

---

[496] Adapted from SK OIPC Review Report F-2006-002 at [23] and [32].
[497] Adapted from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 162.
[498] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition,* Chapter 4 at p. 162.
[499] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-202. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[500] Adapted from Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 402.

agreement is more precise than an "arrangement". Agreements include contracts, memoranda of understanding, collective agreements, etc.[501]

Arrangement is a settlement of mutual relations or claims between parties, an arrangement may or may not be in writing.[502] Arrangements should, whenever possible, be in writing. A verbal arrangement should be the exception. When an arrangement is unwritten, disclosures should be approved at a senior level within the local authority.[503]

Administering is the process of managing something; to provide or arrange something officially as part of one's job.[504]

Enforcing in this context means the act or process of compelling compliance with a law.[505]

Law in this context means a statute.[506]

A **lawful investigation** is an investigation that is authorized or required and permitted by law.[507]

The local authority must be able to identify the legislation under which the investigation is occurring.

The investigation must be active and ongoing or be occurring in the future because of the phrase "carrying out a lawful investigation". If the lawful investigation were concluded, it could not be carried out.

---

[501] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 271.
[502] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-202. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[503] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 271.
[504] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 53.
[505] Adapted from Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 645.
[506] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 1056.
[507] First defined in SK OIPC Review Report 93/021 at p. 6. Adopted in SK OIPC Review Report F-2004-006 at [26] and F-2014-001 at [160].

Agreements concerning the disclosure of personal information by local authorities to other organizations, including federal, provincial, municipal or foreign governments or bodies, should contain:

- A description of the personal information to be collected or disclosed.
- The authority for collecting, using and/or disclosing personal information.
- The purposes for which the personal information is collected, used and/or disclosed.
- A statement of all the administrative, technical, and physical safeguards required to protect the confidentiality of the personal information, especially with respect to its use and disclosure.
- A statement specifying whether information received by a local authority will be subject to the provisions of LA FOIP or, for other jurisdictions where comparable legislation exists, whether that legislation will apply.
- A statement that the disclosure of the personal information will cease if the recipient is discovered to be improperly disclosing the information collected from the local authority.
- The names, titles, and signatures of the officials in both the supplying and receiving organizations who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.[508]

The local authority has discretion under subsection 28(2)(h) of LA FOIP to disclose or not to disclose because of the word "may". In the absence of a requirement in some other legislation or in an agreement, the local authority should be cautious about disclosing personal information when the person or agency requesting it seems to be on a "fishing expedition" and cannot provide definite and focused information as to the nature of the investigation or law being enforced and why the requested information is necessary.[509]

To rely on this provision, the local authority should be able have a copy of any agreement or arrangement in place and be able to identify which law(s) and sections of the law(s) the other party is seeking to administer or enforce. In addition, local authorities should be able to show the connection between the personal information to be disclosed and the administration or enforcement of the law or carrying out the lawful investigation (i.e., there should be a connection between what is being disclosed and the purpose).[510]

---

[508] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at pp. 270 to 271.
[509] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-203. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[510] SK OIPC Investigation Report LA-2010-001 at [27] to [30].

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report LA-2010-001, the Commissioner investigated a complaint involving the City of Saskatoon (City). The complaint alleged that the City disclosed an employee's personal information to the Canada Revenue Agency (CRA). The City asserted it had authority to make the disclosure pursuant to subsection 28(2)(h)(i) of LA FOIP. The City asserted that the CRA administered tax laws for Saskatchewan. The request for personal information came from the Verification and Enforcement Section of the Saskatoon Tax Services Office. The City had a long-standing (more than 27 years) arrangement with the CRA to release information to assist them in administering the tax laws. The Commissioner found that the City failed to meet the burden of proof in demonstrating that subsection 28(2)(h)(i) of LA FOIP provided it with the requisite authority to disclose. The Commissioner noted that the City's submissions to the Commissioner were vague and lacked detail and evidence. The Commissioner stated that in order to rely on this provision, local authorities should be able to provide a copy of any agreement or arrangement in place and be able to identify which law(s) and sections of the law(s) the other party is seeking to administer or enforce. In addition, local authorities should be able to show the connection between the personal information to be disclosed and the administration or enforcement of the law or carrying out the lawful investigation (i.e., there should be a connection between what is being disclosed and the purpose). As such, the Commissioner found that the City could not rely on subsection 28(2)(h)(i) of LA FOIP.

Subsection 28(2)(h.1)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(h.1) for any purpose related to the detection, investigation or prevention of an act or omission that might constitute a terrorist activity as defined in the *Criminal Code*, to:

(i) a government institution;

(ii) the Government of Canada or its agencies, Crown corporations or other institutions;

(iii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iv) the government of a foreign jurisdiction or its institutions;

(v) an international organization of states or its institutions; or

(vi) another local authority;

Subsection 28(2)(h.1) of LA FOIP permits a local authority to disclose personal information about an individual without consent for any purpose related to the detection, investigation or prevention of an act or omission that might constitute a terrorist activity as defined in the *Criminal Code*. For this purpose, the local authority may disclose to any of the enumerated parties listed at subsections 28(2)(h.1)(i) through (vi) of LA FOIP.

The enumerated parties listed include:

(i) A government institution.

For subsection 28(2)(h.1)(i) of LA FOIP to apply, the agency in question must qualify as a *"government institution"*.

Government institution means a "government institution" as defined at subsection 2(1)(d) of *The Freedom of Information and Protection of Privacy Act*. It also includes boards, commissions, Crown corporations and other bodies prescribed in the Appendix, Part I of *The Freedom of Information and Protection of Privacy Regulations*.

(ii) The Government of Canada or its agencies, Crown corporations or other institutions.

For subsection 28(2)(h.1)(ii) of LA FOIP to apply, the agencies in question must qualify as either "*Government of Canada or its agencies, Crown corporations or other institutions*". Because of the possessive pronoun in this clause, "agencies" and "other institutions" should be understood as federal agencies and federal institutions. For "other institutions", it should be either federal government

institutions as defined by the federal *Access to Information Act* or institutions controlled by the federal government.[511]

For some assistance, Schedule 1 (Section 3) of the federal *Access to Information Act* provides a list of federal government institutions.

(iii) The government of another province or territory of Canada, or its agencies, Crown corporations or other institutions.

For subsection 28(2)(h.1)(iii) of LA FOIP to apply, the agencies in question must qualify as a "g*overnment of another province or territory of Canada, or its agencies, Crown corporations or other institutions*". Because of the possessive pronoun in this clause, "agencies" and "other institutions" should be understood as provincial or territorial agencies and institutions. For "other institutions", it should be provincial or territorial government institutions as defined by those provinces and territories.[512]

(iv) The government of a foreign jurisdiction or its institutions.

For subsection 28(2)(h.1)(iv) of LA FOIP to apply, the agency in question must qualify as a "*government of a foreign jurisdiction or its institutions"*. A **foreign jurisdiction** refers to a government or its institutions of any foreign nation or state outside of Canada.[513]

(v) An international organization of states or its institutions.

For subsection 28(2)(h.1)(v) of LA FOIP to apply, the agency in question must qualify as a "*international organization of states or its institutions"*. An **international organization of states** refers to any organization with members representing and acting under the authority of the governments of two or more states. Examples include the United Nations and the International Monetary Fund.[514]

---

[511] SK OIPC Review Report F-2006-002 at [23] and [32].
[512] Adapted from SK OIPC Review Report F-2006-002 at [23] and [32].
[513] Adapted from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 162.
[514] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition,* Chapter 4 at p. 162.

(vi) Another local authority.

> For subsection 28(2)(h.1)(vi) of LA FOIP to apply, the agency in question must qualify as a "*local authority*". Subsection 2(f) *The Local Authority Freedom of Information and Protection of Privacy Act* defines which bodies qualify as local authorities.

This provision uses some similar language and terms as found in subsection 14(1)(a.1) of LA FOIP. Definitions below have been drawn from guidance for this provision in this Chapter and the *Guide to LA FOIP*, Chapter 4: "Exemptions from the Right of Access".

Purpose in this context means the purpose to be attained or the thing intended to be done.[515]

Related to should be given a plain but expansive meaning.[516] The phrase should be read in its grammatical and ordinary sense. There is no need to incorporate complex requirements (such as "substantial connection") for its application, which would be inconsistent with the plain unambiguous meaning of the words of the statute.[517] "*Related to*" requires some connection between the personal information and a purpose related to detecting, investigating, or preventing an act or omission that might constitute a terrorist activity.[518]

Detection is the act of discovering or revealing something that is hidden or barely perceptible, especially to solve a crime.[519]

Investigation can include police, security or administrative investigations or a combination of these. Investigation has been defined, in general terms, as a systematic process of examination, inquiry and observation.[520]

---

[515] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[516] *Gertner v. Lawyers' Professional Indemnity Company,* 2011 ONSC 6121 (CanLII) at [32].
[517] *Ministry of Attorney General and Toronto Star*, 2010 ONSC 991 (CanLII) at [45]. This case dealt specifically with an appeal regarding Ontario's FOIP legislation.
[518] Adapted from *Ministry of Attorney General and Toronto Star*, 2010 ONSC 991 (CanLII) at [43].
[519] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 543.
[520] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 146.

Prevention means the stopping of something, especially something bad, from happening; to hinder or impede.[521] In the context of this provision, it means the stopping of an act or omission that might constitute a terrorist activity.

Omission means a failure to do something.[522] In the context of this provision, it means by failing to do something (e.g., intentionally not stopping an impending known threat to human life in the name of a religious cause), the failure constitutes a terrorist activity.

Terrorist activity is defined at section 83.01 of the *Criminal Code* of Canada. It includes, for example, an act or omission that is committed in or outside Canada that is committed in whole or in part for a political, religious, or ideological purpose, objective, or cause.[523]

The provision uses the phrase "*may constitute a terrorist activity*". It is possible that it may not be definitive that the act or omission has been determined to constitute a terrorist activity at the time of disclosure because detection, investigation or prevention are occurring or are about to occur. Detection, investigation or prevention must be occurring or are about to occur at the time the disclosure occurs.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

[521] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 1380.
[522] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 1260.
[523] *Criminal Code,* R.S.C., 1985, c. C-46, Subsection 83.01(b)(i)(A).

Subsection 28(2)(i)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(i) for the purpose of complying with:

(i) an Act or a regulation;

(ii) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada; or

(iii) a treaty, agreement or arrangement made pursuant to an Act or an Act of the Parliament of Canada;

Subsection 28(2)(i) of LA FOIP permits a local authority to disclose personal information about an individual without consent for the purpose of complying with an Act or regulation of Saskatchewan or Canada or a treaty, agreement or arrangement made pursuant to an Act of Saskatchewan or Canada.

Purpose means the purpose to be attained or the thing intended to be done.[524] In this context, it means to comply as required.

To **comply** with an Act or regulation of Saskatchewan or Canada or a treaty, agreement, or arrangement pursuant to an Act of Saskatchewan or Canada, means to act in accordance with or fulfill the requirements of the Act, regulation, treaty, agreement, or arrangement.[525]

The relevant Act or regulation may not specifically refer to disclosure of personal information.[526] However, the disclosure must be for the purpose of complying with the Act or regulation of Saskatchewan or Canada or the treaty, agreement or arrangement made pursuant to an Act of Saskatchewan or Canada.

---

[524] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[525] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-184. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[526] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-184. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.

Personal information may be disclosed under this provision if the purpose is to comply with:

(i) An Act or a regulation.

> An **Act or a regulation** means an Act of the Legislature together with any regulations issued thereunder and includes an Ordinance of the Northwest Territories in force in Saskatchewan.[527]
>
> The Act or regulation of Saskatchewan may specifically require the disclosure of personal information, or it may not. Either situation fits under this provision. The requirement is that disclosure can occur for the purpose of complying with whatever the Act or regulation requires provided there is a connection between what is being disclosed and what is required to comply. In other words, personal information may be disclosed to enable the local authority to fulfill the requirements of or deliver a service or program or carry out an activity that is authorized by the Act or regulation. Without the disclosure, the aims or objectives of the Act or regulation could not be met.[528]

(ii) An Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada.

> An **Act of the Parliament of Canada or a regulation** encompasses all Acts enacted by the Parliament of Canada together with any regulations issued thereunder.[529]
>
> A federal Act or regulation may specifically require the disclosure of personal information, or it may not. Either situation fits under this provision. The requirement is that disclosure can occur for the purpose of complying with whatever the federal Act or regulation requires provided there is a connection between what is being disclosed and what is required to comply. In other words,

---

[527] See subsection 2-29 of *The Legislation Act*, S.S. 2019, Chapter L-10.2.
[528] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at pp. 6-158 to 6-159. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[529] Office of the Information Commissioner of Canada, *Investigator's Guide to Interpreting the ATIA,* https://www.oic-ci.gc.ca/en/investigators-guide-interpreting-act/section-16-law-enforcement-investigations-security, accessed on June 14, 2019. Definition relied on in SK OIPC Review Report F-2014-001 at [127].

personal information may be disclosed to enable the local authority to fulfill the requirements of or deliver a service or program or carry out an activity that is authorized by a federal Act or regulation. Without the disclosure, the aims or objectives of the federal Act or regulation could not be met.[530]

(iii) A treaty, agreement or arrangement made pursuant to an Act or an Act of the Parliament of Canada.

Treaty is a formally concluded and ratified agreement between states [OED]; a compact made between two or more independent nations with a view to the public welfare; an agreement, league or contract between two or more nations or sovereigns, formally signed by commissioners properly authorized and solemnly ratified by the several sovereigns or the supreme power of each state.[531] For purposes of this provision, the treaty must have been made or entered into pursuant to an Act of Saskatchewan or Canada.

Agreement means a contract between two or more parties creating obligations that are enforceable or otherwise recognizable at law.[532] An agreement is more precise than an "arrangement" although not always in writing. For purposes of this provision, the agreement must have been made or entered into pursuant to an Act of Saskatchewan or Canada. Agreements include contracts, memoranda of understanding, collective agreements, etc.[533]

Example: Under subsection 31(1) of *The Tobacco Tax Act, 1998*, the Minister of Finance may enter into an agreement with the Government of Canada respecting the administration and enforcement of tax payable by importing consumers. Disclosure of personal information by the Minister to the Government of Canada to comply with this agreement would be authorized under the equivalent subsection 29(2)(i)(iii) of *The Freedom of Information and Protection of Privacy Act*.

---

[530] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at pp. 6-158 to 6-159. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[531] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[532] Adapted from Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 402.
[533] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 271.

Agreements concerning the disclosure of personal information by local authorities to other organizations, including federal, provincial, municipal, or foreign governments or bodies, should contain:

- A description of the personal information to be collected or disclosed.
- The authority for collecting, using and/or disclosing personal information.
- The purposes for which the personal information is collected, used and/or disclosed.
- A statement of all the administrative, technical, and physical safeguards required to protect the confidentiality of the personal information, especially with respect to its use and disclosure.
- A statement specifying whether information received by a local authority will be subject to the provisions of LA FOIP or, for other jurisdictions where comparable legislation exists, whether that legislation will apply.
- A statement that the disclosure of the personal information will cease if the recipient is discovered to be improperly disclosing the information collected from the local authority.
- The names, titles, and signatures of the officials in both the supplying and receiving organizations who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.[534]

Arrangement is a settlement of mutual relations or claims between parties.[535] For purposes of this provision, the arrangement must have been made or entered into pursuant to an Act of Saskatchewan or Canada. Arrangements should, whenever possible, be in writing. A verbal arrangement should be the exception. When an arrangement is unwritten, disclosures should be approved at a senior level within the local authority.[536]

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know

[534] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at pp. 270 to 271.
[535] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-202. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[536] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 271.

the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 133-2015, the Commissioner investigated a complaint involving Saskatchewan Power Corporation (SaskPower). The complaint alleged that SaskPower inappropriately disclosed the complainant's personal information and personal health information to the Saskatchewan Workers' Compensation Board (WCB). SaskPower asserted it had authority to disclose the personal information pursuant to various provisions under *The Freedom of Information and Protection of Privacy Act* (FOIP including subsection the equivalent subsection 29(2)(i) of FOIP. SaskPower asserted that subsection 52(f) of *The Workers' Compensation Act, 2013* required SaskPower to disclose the personal information. The Commissioner found that SaskPower was authorized by subsection 29(2)(i)(i) of FOIP to disclose the complainant's personal information to WCB.

Subsection 28(2)(j)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

…

(j) where disclosure is by a law enforcement agency:

(i) to a law enforcement agency in Canada; or

(ii) to a law enforcement agency in a foreign country;

pursuant to an arrangement, a written agreement or treaty or to legislative authority;

Subsection 28(2)(j) of LA FOIP permits a local authority to disclose personal information about an individual without consent where the local authority qualifies as a "law enforcement agency" and the disclosure is to another law enforcement agency in Canada or a foreign country and there is an arrangement, written agreement, treaty or legislative authority to disclose.

There are three criteria that must be considered and met before this provision can be relied upon:

1. Does the local authority that is disclosing, also qualify as a law enforcement agency?

2. Does the agency receiving the personal information qualify as a law enforcement agency in Canada or outside Canada?

3. Is the disclosure being made pursuant to an arrangement, written agreement, treaty, or legislative authority?

1. Does the local authority that is disclosing, also qualify as a law enforcement agency?

It should be noted that subsection 28(2)(g) of LA FOIP addresses disclosure of personal information **to** a law enforcement agency. Subsection 28(2)(j) of LA FOIP addresses disclosure **by** a law enforcement agency (that is also a local authority) to other law enforcement agencies in Canada or abroad.

Therefore, for this provision to apply, the local authority disclosing must also qualify as a "law enforcement agency". In other words, it must meet both definitions (i.e., disclosing and receiving body must be a law enforcement agency). Subsection 28(2) of LA FOIP only applies to local authorities as defined by subsection 2(f) of LA FOIP.

Although section 9 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* defines the bodies that are considered law enforcement agencies and investigative bodies for purposes of subsection 28(2)(g) of LA FOIP, there are several bodies listed that also qualify as local authorities under subsection 2(f) of LA FOIP. Therefore, a starting point could be to check the list at section 9 to see if the local authority disclosing and/or receiving fits under this list. For example, the Regina Police Service would qualify as a law enforcement agency pursuant to subsection 9(b) of the LA FOIP Regulations that could both disclose and receive personal information from another law enforcement agency provided there was an arrangement, written agreement, treaty or legislative authority to do so. Subsection 9(b) of the LA FOIP Regulations provides:

> **9** For purposes of clause 28(2)(g) of the Act, the following law enforcement agencies and investigative bodies are prescribed as law enforcement agencies or investigative bodies to which personal information may be disclosed:
>
> …
>
> (b) a police service or regional police service within the meaning of *The Police Act, 1990*;

2. Does the agency receiving the personal information qualify as a law enforcement agency in Canada or outside Canada?

The local authority/law enforcement agency can disclose personal information to:

(i) Another law enforcement agency in Canada.

(ii) Another law enforcement agency in a foreign country.

A law enforcement agency means an agency primarily engaged in:

- Enforcing an Act or regulation (or enactment).
- Policing.
- Investigations or inspections that could result in a penalty or sanction being imposed or that are otherwise conducted for the purpose of enforcing an Act or regulation (enactment).
- Proceedings that could result in a penalty or sanction being imposed or that are otherwise conducted for the purpose of enforcing an Act or regulation (or enactment).[537]

Again, section 9 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* defines the bodies that are considered law enforcement agencies and investigative bodies for purposes of subsection 28(2)(g) of LA FOIP. Some of those bodies would also qualify as "*law enforcement agencies in Canada*" for purposes of subsection 28(2)(j)(i) of LA FOIP. However, the list is not complete and does not include law enforcement agencies in foreign countries. The above definition for "law enforcement agency" can be relied upon in addition for subsections 28(2)(j)(i) and (ii) of LA FOIP. There may also be Acts or regulations (enactments) in the foreign country that indicate whether the agency being disclosed to qualifies as a "law enforcement agency".

Examples of law enforcement agencies in a foreign country include the Metropolitan Police in England, the Federal Bureau of Investigation and the Unites States Citizenship and Immigration Services and Interpol.[538]

---

[537] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at pp. 6-200 to 6-201. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[538] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 284.

Local authorities should be able to support how the agency being disclosed to qualifies.

3. *Is the disclosure being made pursuant to an arrangement, written agreement, treaty, or legislative authority?*

Disclosure under this provision must be made in accordance with an arrangement, written agreement, treaty or legislative authority.

Arrangement is a settlement of mutual relations or claims between parties. An arrangement may or may not be in writing.[539] Arrangements should, whenever possible, be in writing. A verbal arrangement should be the exception. When an arrangement is unwritten, disclosures should be approved at a senior level within the local authority.[540]

Agreement is a mutual understanding, an arrangement between parties as to a course of action, a contract. An agreement is more precise than an arrangement.[541] For purposes of this provision, the agreement must be in writing. Agreements include contracts, memoranda of understanding, collective agreements, etc.[542]

Treaty is a compact made between two or more independent nations with a view to the public welfare; a binding agreement between states.[543]

Legislative authority means that disclosure of personal information is authorized by some Act or regulation other than LA FOIP.[544]

Agreements concerning the disclosure of personal information by local authorities to other organizations, including federal, provincial, municipal, or foreign governments or bodies, should contain:

---

[539] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-202. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[540] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 271.
[541] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-202. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[542] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 271.
[543] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-202. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[544] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-202. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.

- A description of the personal information to be collected or disclosed.
- The authority for collecting, using and/or disclosing personal information.
- The purposes for which the personal information is collected, used and/or disclosed.
- A statement of all the administrative, technical, and physical safeguards required to protect the confidentiality of the personal information, especially with respect to its use and disclosure.
- A statement specifying whether information received by a local authority will be subject to the provisions of LA FOIP or, for other jurisdictions where comparable legislation exists, whether that legislation will apply.
- A statement that the disclosure of the personal information will cease if the recipient is discovered to be improperly disclosing the information collected from the local authority.
- The names, titles, and signatures of the officials in both the supplying and receiving organizations who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.[545]

A local authority that is a law enforcement agency has a discretion under subsection 28(2)(j) of LA FOIP to disclose or not to disclose personal information to another law enforcement agency. In the absence of a requirement in some other legislation or in an agreement or treaty, a Saskatchewan local authority/law enforcement agency should be cautious about disclosing personal information.

It is recommended that local authorities consult with legal counsel before relying on subsection 28(2)(j) of LA FOIP.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

[545] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at pp. 270 to 271.

Subsection 28(2)(k)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

…

(k) to any person or body for research or statistical purposes if the head:

(i) is satisfied that the purpose for which the information is to be disclosed is not contrary to the public interest and cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates; and

(ii) obtains from the person or body a written agreement not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;

Subsection 28(2)(k) of LA FOIP permits a local authority to disclose personal information about an individual without consent to any person or body for research or statistical purposes if the head of the local authority is satisfied the disclosure is not contrary to the public interest and de-identified information would not reasonably accomplish this purpose. In addition, where there is an agreement in place restricting subsequent disclosures of the identifiable personal information.

Subsection 28(2)(k) of LA FOIP enables research to take place while at the same time ensuring that privacy is protected. This is accomplished by the strict conditions set out in the provision. Prior to disclosing personal information for research or statistical purposes under this provision, the local authority must ensure all criteria are met.

For a local authority to have ability to rely on this provision, the following four criteria must be met:

1. Is the disclosure for research or statistical purposes?

2. Is the "head" satisfied that the disclosure is not contrary to the public interest?

3. Is the "head" satisfied that the purpose cannot be reasonably accomplished with de-identified information?

4. Is there a written agreement in place restricting subsequent disclosures of identifiable personal information?

1. Is the disclosure for research or statistical purposes?

Research means the systematic investigation into and study of materials, sources, etc., to establish facts and reach new conclusions. For a disclosure of personal information for a "**research purpose**" to be permissible, the researcher must intend to use the personal information to investigate and ascertain facts or verify theories.[546]

Statistics is the science of collecting and analyzing numerical data, especially large quantities of data and usually inferring proportions in a whole from proportions in a representative sample, any systematic collection or presentation of such facts. In this context, quantifiable personal information to study trends and draw conclusions.[547]

2. Is the "head" satisfied that the disclosure is not contrary to the public interest?

Contrary means opposite in position or direction; opposite to the proper or right thing; wrong.[548]

Not contrary to the public interest may be understood as not inconsistent with long-term community values, or with the good of society at large.[549]

To determine if something is contrary to the public interest, it is first necessary to understand what public interest is.

---

[546] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020. See also Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at pp. 270 to 296.
[547] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020. See also Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at pp. 270 to 296.
[548] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 509.
[549] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 121.

Public interest means the interest of the general public or of a group of individuals. It does not include the interest of only one individual.[550]

The purpose of a public interest override in LA FOIP (e.g., s. 18(3) and s. 28(2)(n) of LA FOIP) includes promoting democracy by increasing public participation.

A local authority is not required to find that a disclosure promotes a public interest simply that disclosure is not contrary to the public interest. The test for what is "not contrary to the public interest" is different from the test for subsections 18(3) and 28(2)(n)(i) of LA FOIP, which provides for disclosure of information that is in the public interest.[551]

When considering whether subsection 28(2)(k) of LA FOIP can be relied upon, a local authority must consider the circumstances surrounding the request. A local authority may decide that disclosure would be contrary to the public interest based on its knowledge of risks to its clientele or the nature of the request. For example, if the requested information could be used to commit a criminal act or harm an individual or property, then it is likely contrary to the public interest to disclose the information.[552]

The local authority should be able to clearly identify how disclosure is not contrary to the public interest when relying on subsection 28(2)(k) of LA FOIP.

3. Is the "head" satisfied that the purpose cannot be reasonably accomplished with de-identified information?

Information is in *individually identifiable form* if unique identifiers are attached to the information such that the information can identify a particular individual. The identifiers might be an individual's name, address, telephone number, date of birth or social insurance number. Small population cells or contextual information may also allow for the identification of an individual.[553]

---

[550] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed December 15, 2022.
[551] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 121.
[552] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 121.
[553] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 296.

De-identification is the general term for the process of removing personal information from a record or data set.[554]

De-identified information is information that cannot be used to identify an individual, either directly or indirectly. Information is de-identified if it does not identify an individual, and it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual.[555]

Personal information is de-identified through a process involving the removal or modification of both direct identifiers and indirect or quasi-identifiers.[556]

As a best practice, de-identified information should be collected, used and/or disclosed if the purpose for the collection, use and/or disclosure can still be achieved using de-identified information. This isn't always possible. However, local authorities should exercise discretion and consider whether it is possible in each circumstance.

Whether something is **reasonable** is a subjective assessment which means fair, proper, just, moderate, suitable under the circumstances, rational, governed by reason, not immoderate or excessive, the standard which one must observe to avoid liability for negligence, including foreseeable harms.[557] In the context of subsection 28(2)(k) of LA FOIP, the local authority should consider whether the research or statistical purpose can reasonably be accomplished with de-identified information. If the answer is no, then the third criteria is met.

The onus is on the local authority to understand research methods generally and the proposed project specifically, to determine whether identifiable information is truly needed to accomplish the research.

The researcher would submit the research proposal to the local authority in writing, clearly explaining the nature of the research, the information involved and the reason for the request. A detailed proposal enables the local authority to evaluate the necessity for identifiable information, any potential harm to individuals, the academic credentials, skill and

---

[554] ON IPC resource, *De-identification Guidelines for Structured Data,* June 2016 at pp. 1 and 3.
[555] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 3.
[556] ON IPC resource, *De-identification Protocols: Essential for Protecting Privacy*, June 25, 2014 at p. 3.
[557] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed December 15, 2022.

reputation of the researcher, and proposed security for the records containing the information.[558]

4. Is there a written agreement in place restricting subsequent disclosures of identifiable personal information?

Agreement is a mutual understanding, an arrangement between parties as to a course of action, a contract.[559] For purposes of this provision, the agreement must be in writing. Agreements include contracts, memoranda of understanding, etc.[560]

Subsection 28(2)(k) of LA FOIP requires that there be a written agreement in place that restricts a researcher from making subsequent disclosures of the personal information in identifiable form that could reasonably be expected to identify the individual(s) to whom it relates. In addition to this, agreements concerning the disclosure of personal information by local authorities to researchers should contain:

- A description of the personal information to be disclosed.
- The authority for disclosing the personal information.
- The purposes for which the personal information will be collected, used and/or disclosed.
- A statement that clearly restricts any subsequent disclosures of the personal information by the researcher in a form that could reasonably be expected to identify the individuals.
- A statement of all the administrative, technical, and physical safeguards required to protect the confidentiality of the personal information, especially with respect to its use and disclosure.
- A statement specifying whether information received by a local authority will be subject to the provisions of LA FOIP or, for other jurisdictions where comparable legislation exists, whether that legislation will apply.
- A statement that the disclosure of the personal information will cease if the researcher is discovered to be improperly disclosing the information collected from the local authority.

---

[558] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 297.
[559] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-202. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[560] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 271.

- The names, titles, and signatures of the officials in both the supplying and receiving organizations who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.[561]

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Subsection 28(2)(l)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

…

(l) where necessary to protect the mental or physical health or safety of any individual;

Subsection 28(2)(l) of LA FOIP permits a local authority to disclose personal information about an individual without consent where it is necessary to protect the mental or physical health or safety of any individual.

Like other privacy laws in Canada, LA FOIP permits disclosure to protect health and safety. However, it must be "necessary" to protect that health and safety.

[561] Adapted from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at pp. 270 to 271.

Necessary in this context means where the local authority would be unable to protect the mental or physical health or safety of the individual properly or adequately or the group without disclosing the personal information in the proposed manner.[562]

Protect means keep safe from harm or injury.[563]

Safety means the state of being protected from or guarded against hurt or injury; freedom from danger.[564]

Physical health refers to the well-being of an individual's physical body.[565] Determination of the effect of a release of information on an individual's physical health must consider the current or normal state of health of persons who may be affected by the release of information, as well as the decline in health that is expected to occur if the information is disclosed to the applicant. It may be helpful for the head to obtain the assistance of an expert (e.g., a physician) when making this determination.[566]

Physical safety means to be protected from any physical injury or impairment to the human body.[567]

Mental health means the condition of a person in respect of the functioning of the mind.[568] It means the ability of a person's mind to function in its normal state. Determination of the effect of a release of information on a person's mental health must, where practicable, be based on a subjective evaluation made on a case-by-case basis. It may be helpful for the head to obtain the assistance of an expert (e.g., a psychiatrist) when making this determination.[569]

---

[562] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-182. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[563] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 1149.
[564] *The Shorter Oxford English Dictionary on Historical Principles*, Oxford University Press 1973, Volume 2 at p. 2647.
[565] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 137.
[566] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[567] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 861.
[568] *The Shorter Oxford English Dictionary on Historical Principles*, Oxford University Press 1973, Volume 1 at p. 1220.
[569] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

The decision to disclose must be made on a case-by-case basis, and the decision must be made carefully and sensitively. But privacy laws do not stand in the way of a local authority disclosing personal information where necessary to protect an individual or the public. In the words of the Ontario and British Columbia Information and Privacy Commissioners, sometimes "life trumps privacy, and our laws reflect that reality".[570]

Examples:

- Disclosure of personal information about a dangerous offender being released from a correctional institution.
- Disclosure to another local authority or agency that a client is known to behave violently toward employees when the other local authority or agency is likely to encounter this client, so appropriate precautions may be taken to protect employees (such as arranging for the presence of a security guard, etc.).

Local authorities should still abide by the data minimization and need to know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need to know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 107-2014, the Commissioner investigated a complaint involving the Saskatchewan Research Council (SRC). The complaint alleged that SRC sent emails to SRC staff and board members advising employees that the complainant intended to commence a lawsuit against SRC and that he had submitted access to information requests. The emails indicated that if the complainant showed up at SRC, staff should ask him to leave and advise him he is only to communicate through SRC legal counsel. The emails also stated that if staff felt threatened or he refused to leave to contact police. SRC asserted that it had authority to disclose the personal information pursuant to the equivalent provision in *The Freedom of*

[570] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-182. Available at Chapter (gov.mb.ca). Accessed December 15, 2022. Quote of Commissioner also from Manitoba resource but originated from *Practice Tools for Exercising Discretion: Emergency Disclosure of Personal Information by Universities, Colleges and other Educational Institutions*, October 2008, page 1. This joint paper of the Ontario and B.C. IPC's and can be found on the ON IPC website at: 1464 (oipc.bc.ca).

Information and Protection of Privacy Act (FOIP) - subsection 29(2)(m). The Commissioner found that SRC was authorized to disclose the opinion about the complainant (that he posed a threat) and the photograph of the complainant pursuant to subsection 29(2)(m) of FOIP. However, the Commissioner also found that SRC was not authorized to use or disclose the other personal information of the complainant.

In Investigation Report 282-2018, the Commissioner investigated an alleged breach of privacy involving the Rural Municipality of Parkdale (RM). The complaint alleged that the RM disclosed the personal information of a deceased individual in its council meeting minutes which were posted to the RM's website. The RM asserted it had authority to disclose the personal information pursuant to several provisions of subsection 28(2) of LA FOIP including subsection 28(2)(l) of LA FOIP. Upon investigation, the Commissioner was not convinced that the RM had demonstrated how the public knowing the deceased's personal information was necessary to prevent harm from coming to others. As such, the Commissioner found the RM could not rely on subsection 28(2)(l) of LA FOIP for the disclosure.

In Investigation Report 322-2017, 120-2018, the Commissioner investigated a proactively reported breach of privacy involving Saskatchewan Legal Aid Commission (Legal Aid) and the Ministry of Corrections and Policing (Corrections). The breach involved an employee at the Saskatoon Correctional Centre disclosing personal information about an individual in custody at the Saskatoon Correctional Centre (SCC) to a Legal Aid employee. Legal Aid and Corrections both asserted the disclosure was authorized pursuant to the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP) - subsection 29(2)(m). The Commissioner determined that the disclosure was not authorized by subsection 29(2)(m) of FOIP.

In Investigation Report 027-2022, the Commissioner investigated a complaint involving the Ministry of SaskBuilds and Procurement (SaskBuilds). The complaint alleged that SaskBuilds had disclosed the complainant's personal information without authority to Transport Canada and the complainant's physician. SaskBuilds asserted that it had authority for the disclosure pursuant to various provisions including the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP) - subsection 29(2)(m). The complainant was an employee of SaskBuilds and was taking training sessions. The information disclosed to Transport Canada pertained to the medical condition of the complainant which SaskBuilds asserted that the medical condition may have affected the physical health or safety of program staff and others. The Commissioner found that subsection 29(2)(m) of FOIP provided authority for SaskBuilds to disclose the complainant's personal information to Transport Canada and their physician.

Subsection 28(2)(m)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(m) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;

Subsection 28(2)(m) of LA FOIP permits a local authority to disclose personal information about an individual without consent in certain compassionate circumstances.

The compassionate circumstances that must exist for this provision to apply include:

1. The purpose for the disclosure must be to facilitate contact for the individual with their next of kin or a friend.

2. The individual must be injured, ill or deceased

1. Is the purpose of the disclosure to facilitate contact for the individual with their next of kin or a friend?

Facilitate means to make easier or less difficult.[571]

Next of kin is a person's nearest relative by blood or marriage which could include: a cousin, grandparent, niece, or nephew, who has close ties to the individual who is injured, ill or deceased. For example:

- Spouse, parent, child.
- Cousins brought up together as siblings.
- A grandchild brought up by grandparents.[572]

---

[571] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[572] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Friend is a person with whom one has a bond of mutual affection, typically one exclusive of sexual or family relations.[573] It includes someone that has a close personal relationship with the individual.

2. Is the individual injured, ill, or deceased?

The subsection is very specific that to rely on this provision, the individual whose personal information is being disclosed to facilitate contact must be either injured, ill or deceased.

Injured physically harmed or wounded.[574]

To be ill means to not be in full health; unwell.[575]

Deceased means no longer alive.[576]

Local authorities should exercise caution in making sure that the disclosure under subsection 28(2)(m) of LA FOIP is not contrary to the expressed wishes of the individual. For example, where the individual has expressly stated they do not want to have contact with a particular family member.

This provision does not permit the disclosure of the nature of the illness, injury, or death.[577] Such information is "personal health information" and can only be disclosed in accordance with *The Health Information Protection Act* (HIPA). See *Subsection 23(1.1)* earlier in this Chapter for assistance on whether HIPA applies. For an example under HIPA of a provision that might apply, see subsection 27(2)(c) of HIPA.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

---

[573] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 566.
[574] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 729.
[575] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 707.
[576] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 367.
[577] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-215. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Subsection 28(2)(n)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(n) for any purpose where, in the opinion of the head:

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or

(ii) disclosure would clearly benefit the individual to whom the information relates;

Subsection 28(2)(n) of LA FOIP permits a local authority to disclose personal information about an individual without consent for any purpose where one of the enumerated circumstances exists.

To rely on this provision, one of the following two circumstances must exist:

- The public interest in disclosure clearly outweighs any invasion of privacy that could result from disclosure; or
- Disclosure would clearly benefit the individual to whom the information relates.

Subsection 28(2)(n)(i)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(n) for any purpose where, in the opinion of the head:

> (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or

Subsection 28(2)(n)(i) of LA FOIP provides that a local authority can disclose personal information about an individual without consent for any purpose where the public interest in disclosure clearly outweighs any invasion of privacy that could result from disclosure.

This provision requires the exercise of discretion by the "head" of the local authority.

Disclosure can be for any purpose provided the criteria in subsection 28(2)(n)(i) of LA FOIP are met.

The following test can be applied to assist with determining whether to rely on this provision:

1. Is the information "personal information" as defined by LA FOIP?

2. Is there a public interest in the personal information?

3. Does the public interest clearly outweigh any invasion of privacy?[578]

1. Is the information "personal information" as defined by LA FOIP?

Section 23 of LA FOIP defines "personal information". See *Section 23* earlier in this Chapter.

2. Is there a public interest in the personal information?

Public interest means the interest of the general public or of a group of individuals. It does not include the interest of only one individual.[579]

The criteria for assessing whether there is a public interest in information are as follows:[580]

---

[578] This three-part test was established in SK OIPC Review Report 082-2017 at [26]. The report dealt with the equivalent provision in *The Local Authority Freedom of Information and Protection of Privacy Act*, section 28(2)(n)(i). It was adopted for purposes of subsection 29(2)(o)(i) of FOIP in Review Report 173-2018 at [22].

[579] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed December 15, 2022.

[580] This criteria was first adopted in SK OIPC Review Report 173-2018 at [23].

(1) Will the records contribute to the public understanding of, or to debate on or resolution of, a matter or issue that is of concern to the public or a sector of the public, or that would be, if the public knew about it? The following may be relevant:

- Have others besides the applicant sought or expressed an interest in the records?
- Are there other indicators that the public has or would have an interest in the records?

(2) Is the applicant motivated by commercial or other private interests or purposes, or by a concern on behalf of the public, or a sector of the public? The following may be relevant:

- Do the records relate to a personal conflict between the applicant and the local authority?
- What is the likelihood the applicant will disseminate the contents of the records in a manner that will benefit the public?

(3) If the records are about the process or functioning of the local authority, will they contribute to open, transparent, and accountable government? The following may be relevant:

- Do the records contain information that will show how the local authority reached or will reach a decision?
- Are the records desirable for subjecting the activities of the local authority to scrutiny?
- Will the records shed light on an activity of the local authority that have been called into question?[581]

The purpose of a public interest override such as subsection 28(2)(n)(i) of LA FOIP includes promoting democracy by increasing public participation.

When considering the public interest, the local authority should create a list of factors in favour of withholding and public interest factors for releasing. This will help when it comes to

[581] These criteria were first adopted in SK OIPC Review Report 173-2018 at [23].

assessing the relative weight of the factors and whether disclosing is in the public interest.[582] What are the benefits to be derived from disclosing?

LA FOIP's central purpose is to shed light on the operations of local authorities and to promote democracy. Consider whether disclosure of the personal information serves to inform or enlighten the citizenry about the activities of their government. Also consider if disclosure adds in some way to information the public already has to make effective use of the means of expressing public opinion or to make political choices.

A public interest does not exist where the interests being advanced are essentially private in nature. However, where a private interest in disclosure raises issues of a more general application, a public interest may be found to exist.

A public interest is not automatically established where the media is involved.

To be in the public interest, the personal information must relate to a matter of compelling public interest, and not just be of interest or of curiosity to the public, a group of people or individuals. What constitutes a compelling public interest is defined narrowly.[583] The following are some examples where disclosure may be in the public interest:

- An individual is the carrier of a contagious or dangerous disease.
- A violent or dangerous offender has been released into the community.
- An individual is seeking employment in childcare based on a false resume is found to have a history of child molestation that is recorded.
- Information has come to light about corruption or serious misuse of public funds.[584]

The local authority should be able to identify what the public interest would be.

3. Does the public interest clearly outweigh any invasion of privacy?

Where a public interest has been established, the local authority must then weigh the public interest against the personal privacy interests of the individual whose personal information

---

[582] Adapted from the Office of the Newfoundland and Labrador Information and Privacy Commissioner (NFLD IPC), Resource, *Guidelines for Public Interest Override* at pp. 2 and 3.
[583] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 6, "Disclosure in the Public Interest" at p. 229.
[584] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 6, "Disclosure in the Public Interest" at p. 229.

may be disclosed pursuant to subsection 28(2)(n)(i) of LA FOIP. To rely on the provision, the public interest must clearly outweigh any invasion of privacy.

Clearly means visible, unmistakable, beyond a question or beyond a reasonable doubt; honestly, straightforwardly, and frankly; plainly.[585]

Outweigh means to be of more importance or value than something else.[586]

Invasion of privacy is a term that means the privacy of a person has been invaded.[587] *Invasion* means an encroachment upon the rights of another.[588]

Some further things to consider when weighing the public interest:

- Is there another public process or forum established to address public interest considerations.
- Has a significant amount of information already been disclosed and is it adequate to address any public interest considerations.
- Is there already wide public coverage or debate of the issue and disclosing the records would not shed further light on the matter.

Some things to consider when weighing any invasion of privacy:

- Consider the representations made by the affected individual(s) arguing against disclosure.
    - Note that notification to the affected individual is required prior to disclosure pursuant to subsection 33(1)(b) of LA FOIP. An affected individual that is provided notice, has the right to make representations to the local authority as to why their personal information should not be disclosed. For more on this process see *Guide to LA FOIP*, Chapter 5 – "Third Party Information".

---

[585] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[586] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1330.
[587] The Law Dictionary, Black's Law Dictionary, Free 2nd ed. Available at INVASION OF PRIVACY Definition & Meaning - Black's Law Dictionary (thelawdictionary.org).
[588] The Law Dictionary, Black's Law Dictionary, Free 2nd ed. Available at INVASION Definition & Meaning - Black's Law Dictionary (thelawdictionary.org).

- Should the affected individual's privacy rights be given preference over the public interest that exists?

Local authorities should apply the "invasion-of-privacy" test to determine the level of privacy risk in the disclosure. It involves a detailed review of three interrelated risk factors that will help local authorities determine whether to rely on subsection 28(2)(n)(i) of LA FOIP. These three factors are the sensitivity of the information; the expectations of the individual; and the probability and degree of injury. In addition, local authorities should consider factors unique to their own operational context, as applicable:[589]

(1) Sensitivity of the information

- Consider whether the type of information is of a detailed (e.g., name and address) or highly personal (e.g., health information) nature.
- Evaluate the context in which the information was collected and determine whether any contextual sensitivities apply to the information. For example, a list of public servants may not be considered particularly sensitive, but that same list, if collected to identify employees having a specific illness would be considered sensitive based on the context.

(2) Expectations of the individual

- Evaluate the conditions under which the personal information was collected and consider what expectations the collecting institution may have established for its confidentiality, including whether the possibility of disclosure is conveyed in an applicable Privacy Notice Statement.
- Consider the reasonable expectations of privacy that apply to the context in which the information was collected. To determine what constitutes a reasonable expectation of privacy, courts will look at the totality of circumstances. This could include location of collection (e.g., in a private conversation as compared to a public town hall), context of collection (e.g., in a routine application for services as compared to a letter sent to several local authorities), etc.

[589] Adapted from Privacy Commissioner of Canada, *Public Interest Disclosures by federal institutions under the Privacy Act*, revised June 2022. Available at Public interest disclosures by federal institutions under the Privacy Act - Office of the Privacy Commissioner of Canada. Accessed December 15, 2022.

(3) Probability and degree of injury

- Consider the probability and degree or gravity of injury relative to the benefits of the disclosure to the public. This could include personal or physical injury, or damage to the reputation of an individual or others, which causes adverse consequences (e.g., any harm or embarrassment that negatively affects an individual's career, reputation, financial position, safety, health, or well-being).
- Determine the potential of injury if the receiving party wrongfully disclosed the information further.[590]

Where the local authority intends to rely on this provision to disclose personal information, notification is required to the individual(s) pursuant to the third party notification requirements outlined at subsection 33(1)(b) of LA FOIP. For more on this process, see the *Guide to LA FOIP*, Chapter 5 – "Third Party Information".

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 092-2015 to 095-2015, the Commissioner investigated an alleged breach of privacy involving the Ministry of Health, the Office of the Premier, Oliver Lodge and Saskatoon Regional Health Authority. The investigation involved the collection and disclosure of a care aide's personal information. The Commissioner found that there was a public interest in the release of the information and that the public interest outweighed any invasion of privacy.

In Review Report 282-2018, the Commissioner investigated an alleged breach of privacy involving the Rural Municipality of Parkdale (RM). The complaint alleged the RM disclosed a former employee's personal information who was deceased. The disclosure was made by posting the personal information in council meeting minutes which were posted to the RM's website. Along with other provisions, the RM asserted it had authority to disclose the

[590] Privacy Commissioner of Canada, *Public Interest Disclosures by federal institutions under the Privacy Act*, revised June 2022. Available at Public interest disclosures by federal institutions under the Privacy Act - Office of the Privacy Commissioner of Canada. Accessed December 15, 2022.

personal information pursuant to subsection 28(2)(n) of LA FOIP. The Commissioner found that the RM did not provide supporting arguments or explain how subsection 28(2)(n) of LA FOIP applied in the circumstances. Therefore, the Commissioner found that the RM could not rely on subsection 28(2)(n) of LA FOIP for the disclosure.

In Investigation Report 082-2017, the Commissioner reviewed the Rural Municipality of McKillop No. 220 (RM). An applicant requested access to invoices submitted to the RM for contract services by a former employee including invoices submitted by summer students. The RM withheld all and portions of records asserting the records contained personal information citing subsection 28(1) of LA FOIP. Upon review, the Commissioner decided to consider whether release of the financial transactions involving the RM and the former employee was in the public interest pursuant to subsection 28(2)(n)(i) of LA FOIP. The Commissioner's office provided notice of the review to the former employee pursuant to subsection 41(1)(a) of LA FOIP and advised the former employee of the Commissioner's intention to review the applicability of subsection 28(2)(n)(i) of LA FOIP. After considering the three part test for this provision, the Commissioner recommended the RM consider disclosing the personal information pursuant to subsection 28(2)(n)(i) of LA FOIP.

In Review Report 173-2018, the Commissioner reviewed a denial of access by Meewasin Valley Authority (MVA). An applicant was denied access to the amount of the severance package for an individual from MVA. The Commissioner found that the information qualified as the employee's personal information pursuant to subsection 24(1)(b) of *The Freedom of Information and Protection of Privacy Act* (FOIP). However, the Commissioner advised MVA that it had the discretionary ability to disclose the personal information pursuant to the equivalent provision in FOIP - subsections 29(2)(o)(i) and 16(g)(ii) of *The Freedom of Information and Protection of Privacy Regulations* (equivalent to subsection 10(g)(ii) of the LA FOIP Regulations). The Commissioner recommended MVA consider subsection 29(2)(o) of FOIP.

In Review Report 082-2019, 083-2019, the Commissioner reviewed a denial of access by the Ministry of Health (Health). An applicant was denied access to the names of physicians, their specialties and total payment amounts they received for 2018 (top 100 physician billers and all physicians that billed the medical system more than $1 million). The Commissioner found that none of the exemptions applied by Health to the information qualified. The Commissioner recommended Health consider releasing the information under subsection 29(2)(o) of FOIP.

In Review Report 342-2019, the Commissioner reviewed a denial of access by the Ministry of Health (Health). An applicant was denied access to the names of the top 10 physicians, their

specialties, total payment amounts received for 2018 and the name of the city where the physician's practice was located. The Commissioner found that none of the exemptions applied by Health to the information qualified. The Commissioner recommended Health consider releasing the information under subsection 29(2)(o) of FOIP.

In Review Report 035-2019, the Commissioner reviewed a denial of access by the City of Saskatoon (City). The City denied access to lump sum payment amounts paid to its employees. The Commissioner recommended the City of Saskatoon consider subsection 28(2)(n)(i) of LA FOIP.

Subsection 28(2)(n)(ii)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(n) for any purpose where, in the opinion of the head:

...

(ii) disclosure would clearly benefit the individual to whom the information relates;

Subsection 28(2)(n)(ii) of LA FOIP permits a local authority to disclose personal information about an individual without consent where the disclosure would clearly benefit the individual.

Clearly means visible, unmistakable, beyond a question or beyond a reasonable doubt; honestly, straightforwardly, and frankly; plainly.[591]

Benefit means a favourable or helpful factor or circumstance; advantage, profit.[592]

[591] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[592] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 162-2020, the Commissioner investigated a privacy complaint involving the Water Security Agency (WSA). The complaint alleged that the WSA disclosed the complainant's personal information to the Town of Radisson. The WSA asserted it had authority to disclose the personal information pursuant to the equivalent subsection 29(2)(o)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP). The Commissioner found that the WSA did not demonstrate that the disclosure would clearly benefit the individual. As such, the Commissioner found that subsection 29(2)(o)(ii) of FOIP did not provide authority for the disclosure.

Subsection 28(2)(o)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(o) to the Government of Canada or the Government of Saskatchewan to facilitate the auditing of shared cost programs;

Subsection 28(2)(o) of LA FOIP permits a local authority to disclose personal information about an individual without consent if it is to the Government of Canada or the Government of Saskatchewan to facilitate the auditing of shared cost programs.

Government of Canada means the Crown in right of Canada.[593]

Government of Saskatchewan means the Crown in right of Saskatchewan.[594]

[593] *The Legislation Act*, SS 2019, c L-10.2 at s. 2-29.
[594] *The Legislation Act*, SS 2019, c L-10.2 at s. 2-29.

Facilitate means to make easier or less difficult.[595]

An **audit** in this context is an official examination of accounts or a systematic review of the activities of a shared cost program of the Government of Canada or the Government of Saskatchewan.[596]

Shared cost programs are programs where the cost is shared among different parties including federal, provincial, and municipal governments. Through cost sharing, funding is provided by the federal or provincial government towards projects (e.g., infrastructure projects) and is matched by other partners, such as provinces, territories, municipalities, or the private sector.[597]

Examples of cost-sharing programs can include (but are not limited to):

- Parks Canada's National Cost Sharing Program for Heritage Places which helps ensure the protection of heritage places.
- Infrastructure Canada's 2014 New Building Canada Fund to support investing in infrastructure across Canada.
- Canadian Agricultural Partnership (CAP) which is a five-year investment by federal and provincial governments in strategic initiatives for Saskatchewan agriculture.

There is often a cost sharing agreement in place that establishes the parties and the amount each party will contribute to the shared cost program.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

---

[595] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[596] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-173. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[597] Government of Canada, Infrastructure Canada, *Cost-Sharing: Supporting more projects with every dollar*. Available at Infrastructure Canada - Cost-Sharing: Supporting more projects with every dollar. Accessed on February 16, 2023.

Subsection 28(2)(p)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(p) if the information is publicly available, including information that is prescribed as publicly available;

Subsection 28(2)(p) of LA FOIP permits a local authority to disclose personal information about an individual without consent if the information is publicly available, including information that is prescribed in *The Local Authority Freedom of Information and Protection of Privacy Regulations* as publicly available. Subsection 2(i) of LA FOIP provides:

2 In this Act:

...

(i) **"prescribed"** means prescribed in the regulations;

At the time of this Chapter being issued, *The Local Authority Freedom of Information and Protection of Privacy Regulations* did not have a provision that prescribed any information as "publicly available". However, subsection 28(2)(p) of LA FOIP is an amendment to LA FOIP that came into force on January 1, 2018 so this could change in the future.

Publicly available means published material, material that is a matter of public record (for example, through a public registry).[598]

Published material is material that is made known to people in general, an advising of the public or making known of something to the public for a purpose.[599]

Public record is defined as a record that a government unit is required by law to keep, such as land deeds kept at a county courthouse. Public records are generally open to view by the public.[600]

---

[598] SK OIPC Review Report LA-2012-004 at [11].
[599] SK OIPC Review Report 249-2017 at [7].
[600] Garner, Bryan A., 2004. *Black's Law Dictionary, 8th Edition*. St. Paul, Minn.: West Group at p. 1301, relied on in *Germain v. Automobile Injury Appeal Commission,* 2009 SKKB 106 (CanLII) at [69] and [72]. Also cited in SK OIPC Investigation Report LA-2012-001 at [14] to [17].

The local authority should assess how public the information really is. Factors such as the circumstances in which the information was released to the public or the media, when it was released, and how much information is properly in the public realm will be relevant.[601]

For example, a local authority should not automatically treat personal information about an individual as public and freely disclose it to others simply because the information has been published in some form in the media or in a report that has been made public. Depending on the circumstances of the publication, further disclosure may result in a breach of privacy and may even expose the local authority to legal liability (e.g., to a civil suit for defamation).[602]

"It goes without saying that by appearing in public, an individual does not automatically forfeit his or her interest in retaining control over the personal information which is thereby exposed."[603]

If relying on this provision to disclose personal information, it is recommended that legal counsel be consulted.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 282-2018, the Commissioner investigated an alleged breach of privacy involving the Rural Municipality of Parkdale (RM). The complaint alleged that the RM disclosed in meeting minutes that were published to its website, the personal information of a deceased employee in relation to an appeal of compensation benefits the RM was undertaking. Along with other provisions, the RM asserted it had authority to disclose the personal information pursuant to subsection 28(2)(p) of LA FOIP. Although the RM provided copies of five news articles it did not specifically demonstrate how the personal information

[601] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-219. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[602] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-219. Available at Chapter (gov.mb.ca). Accessed December 15, 2022.
[603] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers*, Local 401, 2013 SCC 62 (CanLII), [2013] 3 SCR 733, at [27].

of the deceased that was disclosed was linked to the media articles. The data elements would have to match up between what was disclosed and what was alleged to be publicly available via the media articles. However, the RM did not provide this. Therefore, the Commissioner found that the RM could not rely on subsection 28(2)(p) of LA FOIP for the disclosure.

Subsection 28(2)(q)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(q) to the commissioner;

Subsection 28(2)(q) of LA FOIP permits a local authority to disclose personal information about an individual without consent to the Saskatchewan Information and Privacy Commissioner.

The Saskatchewan Information and Privacy Commissioner is an independent Officer of the Legislative Assembly of Saskatchewan. The Office of the Saskatchewan Information and Privacy Commissioner (SK OIPC) investigates privacy complaints involving government institutions, local authorities and health trustees. It also reviews denials of access to information including personal information. To fulfill its mandate, the SK OIPC may need personal information from a local authority.

A local authority may disclose personal information without consent to the SK OIPC provided it is for the purpose of enabling performance of the duties of the Commissioner.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Subsection 28(2)(r)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

…

(r) for any purpose in accordance with any Act or regulation that authorizes disclosure;

Subsection 28(2)(r) of LA FOIP permits a local authority to disclose personal information about an individual without consent for any purpose in accordance with an Act or regulation that authorizes disclosure.

Purpose means the purpose for which personal information is being obtained or compiled, the object to be attained or the thing intended to be done, e.g., the administration of a program, the provision of a service or other activity.[604]

An **Act or a regulation** means an Act of the Legislature together with any regulations issued thereunder and includes an Ordinance of the Northwest Territories in force in Saskatchewan.[605] It does not include Acts or regulations in other jurisdictions.

To **authorize** means to give official permission to do something; sanction or warrant; to formally approve.[606]

The Act or regulation of Saskatchewan may specifically require the disclosure of personal information, or it may simply "authorize" it. Either situation fits under this provision. However, if the Act or regulation requires disclosure, subsection 28(2)(i)(i) of LA FOIP may also provide authority to disclose.

---

[604] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[605] See subsection 2-29 of *The Legislation Act*, S.S. 2019, Chapter L-10.2.
[606] Garner, Bryan A., 2009. *Black's Law Dictionary, Deluxe 10th Edition*. St. Paul, Minn.: West Group at p. 165.

If disclosure of personal information is "authorized" – but not required – by an Act or regulation, the local authority has more discretion as to whether to disclose the information.[607]

Subsection 28(2)(r) of LA FOIP provides that disclosure can occur for any purpose provided the other Act or regulation "authorizes" disclosure of personal information. Purposes can include, but is not limited to, enabling the other local authority, person, or organization to fulfill the requirements of, deliver a service or program or carry out an activity that is authorized by the Act or regulation. Without the disclosure, the aims or objectives of the Act or regulation may not be met.[608]

The personal information disclosed and the authorizing provision in the other Act or regulation should have a connection. The local authority must ensure that the disclosure is strictly in compliance with the Act or regulation that authorizes the disclosure.[609] The personal information must be relevant for the purpose.

Before disclosing personal information under subsection 28(2)(r) of LA FOIP in response to a request, a local authority should ask the receiving party to provide their legal authority for collecting the information. A local authority requesting personal information from another local authority should be able to provide the disclosing local authority with its legal authority for collecting the information.[610]

Example:

Section 20 of *The Correctional Services Regulations, 2013* authorizes use and disclosure of any information as follows:

> **Use or disclosure of information**
> **20** Any information obtained from inmate communication, including information obtained as a result of the monitoring of inmate communication or the interception, opening or examination of mail, may be used or disclosed:

---

[607] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 272.
[608] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at pp. 6-158 to 6-159. Available at Chapter (gov.mb.ca). Accessed December 14, 2022.
[609] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 272.
[610] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 273.

(a) for the purposes of protecting the security of the correctional facility or the safety of inmates, staff members or the public;

(b) for the purposes of the investigation of or prevention of the commission of an offence;

(c) for the purposes of any investigation being conducted pursuant to the Act; or

(d) for any purpose for which personal information may be used or disclosed by a government institution pursuant to *The Freedom of Information and Protection of Privacy Act*.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 237-2016, the Commissioner investigated an alleged breach of privacy involving the Rural Municipality of Rosthern (RM). The complaint alleged that the RM disclosed an individual's personal information by posting it in the council's meeting minutes which then went on the RM's website. The Commissioner found that the RM had authority to disclose the personal information pursuant to subsection 28(2)(r) of LA FOIP and subsection 117(1)(d) of *The Municipalities Act*. However, the Commissioner made several recommendations to protect personal information while still making council meeting minutes publicly available. The recommendations included: providing public notice to residents about how personal information can become part of the agenda and published on the website, redact sensitive personal information when distributing information for council meetings, consider closing the meeting when sensitive personal information will be discussed, put the least amount of personal information in the meeting minutes (e.g., remove names, or use initials), and to follow these recommendations before posting minutes to the website.

Subsection 28(2)(s)

Disclosure of personal information

28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

...

(s) as prescribed in the regulations.

Subsection 28(2)(s) of LA FOIP permits a local authority to disclose personal information about an individual without consent if disclosure is prescribed in *The Local Authority Freedom of Information and Protection of Privacy Regulations*. Subsection 2(i) of LA FOIP provides:

2 In this Act:

...

(i) **"prescribed"** means prescribed in the regulations;

There are three provisions in *The Local Authority Freedom of Information and Protection of Privacy Regulations* which are prescribed pursuant to subsection 28(2)(s) of LA FOIP and permit additional disclosures not covered in LA FOIP. These three provisions are as follows:

1. Section 10 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* provides for "Other" disclosures of personal information for purposes of subsection 28(2)(s) of LA FOIP. These other disclosures can be found at subsections 10(a) through (n) of *The Local Authority Freedom of Information and Protection of Privacy Regulations*.

2. Section 10.1 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* provides for disclosures of personal information in accordance with an "information sharing agreement entered into under *The Freedom of Information and Protection of Privacy Regulations* or *The Health Information Protection Regulations* to a party involved in delivering a common or integrated service" if it is for the purpose of assessing, planning or delivering the common or integrated service. For more on common or integrated services see section 17.1 of *The Freedom of Information and Protection of Privacy Regulations* or section 5.2 of *The Health Information Protection Regulations*.

3. Section 10.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* provides for the disclosure of the name of a deceased person to the public by a police service or regional police service if the person's death is being investigated as a homicide by the police service or regional police service.

The SK OIPC plans to develop a resource or appendix that will provide guidance on all the various disclosure provisions in *The Local Authority Freedom of Information and Protection of Privacy Regulations* prescribed pursuant to subsection 28(2)(s) of LA FOIP.

When relying on authority pursuant to subsection 28(2)(s) of LA FOIP, local authorities should point to both subsection 28(2)(s) of LA FOIP and the specific subsection in *The Local Authority Freedom of Information and Protection of Privacy Regulations* that provides the authority. For example, authority can be referred to as follows:

> Subsection 28(2)(s) of LA FOIP and section 10.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* provides that a police service or a regional police service as defined in *The Police Act, 1990*, may disclose to the public the name of a deceased person if the death is being investigated as a homicide by the police service or regional police service:
>
> > **28**(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:
> >
> > …
> >
> > (s) as prescribed in the regulations.
>
> > **10.2** For the purposes of clause 28(2)(s) of the Act, a police service or regional police service as defined in *The Police Act, 1990* may disclose to the public the name of a deceased person if the person's death is being investigated as a homicide by the police service or regional police service.

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

IPC Findings

In Investigation Report 062-2016, the Commissioner investigated an alleged breach of privacy involving the former Keewatin Yatthe Regional Health Authority (Keewatin). The complaint alleged that Keewatin disclosed the complainant's personal information to the Saskatchewan Union of Nurses (SUN) and the Saskatchewan Association of Health Organizations (SAHO). The personal information pertained to the performance of the employee and their misconduct. Keewatin asserted that subsection 28(2)(s) of LA FOIP provided authority for the disclosure and pointed to subsection 10(b) and (f) of *The Local Authority Freedom of Information and Protection of Privacy Regulations.* The Commissioner found that Keewatin had authority for the disclosure pursuant to subsection 28(2)(s) of LA FOIP and subsections 10(b) and (f) of *The Local Authority Freedom of Information and Protection of Privacy Regulations.*

In Investigation Report 296-2017, the Commissioner investigated an alleged breach of privacy involving the Northern Lights School Division No. 113 (Northern Lights). The complaint alleged that Northern Lights disclosed a letter of termination to the complainant's new employer without authority to do so. Northern Lights asserted it had authority to do so under subsection 28(2)(s) of LA FOIP and subsection 10(g)(ii) of *The Local Authority Freedom of Information and Protection of Privacy Regulations.* The Commissioner found that Northern Lights had authority under subsection 28(2)(s) of LA FOIP and subsection 10(g)(ii) of *The Local Authority Freedom of Information and Protection of Privacy Regulations.*

Section 28.1: Notification

Notification

28.1 A local authority shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

Section 28.1 of LA FOIP places an obligation on a local authority to notify individuals when their personal information has been breached and a real risk of significant harm exists for the affected individual.

Reasonable steps - whether something is **reasonable** is a subjective assessment which means fair, proper, just, moderate, suitable under the circumstances, rational, governed by

reason, not immoderate or excessive, the standard which one must observe to avoid liability for negligence, including foreseeable harms.[611]

Notify means to inform affected individual(s). For this provision, notification can occur quickly by telephone or in-person so the individual(s) can take immediate steps to protect themselves (e.g., change passwords, contact financial institutions, etc.) but should be followed up with notification in writing.

Even where section 28.1 of LA FOIP does not apply, unless there is a compelling reason not to, local authorities should always notify affected individuals of a privacy breach.[612] Affected individuals are in the best position to determine how a privacy breach will affect them.[613]

Notification to affected individuals should include the following information:

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may come to them because of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.[614]

Unauthorized use or disclosure is one that does not comply with Part IV of LA FOIP. Part IV of LA FOIP contains the privacy provisions related to a local authority's handling of personal information of individuals.

---

[611] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed December 15, 2022.
[612] SK OIPC Investigation Report 088-2022 at [23].
[613] SK OIPC Investigation Report 370-2021 at [19].
[614] SK OIPC resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities* at p. 6, available at Privacy Breach Guidelines (oipc.sk.ca). Accessed December 16, 2022.

Reasonable in the circumstances - whether something is **reasonable** is a subjective assessment which means fair, proper, just, moderate, suitable under the circumstances, rational, governed by reason, not immoderate or excessive, the standard which one must observe to avoid liability for negligence, including foreseeable harms.[615]

Real risk of significant harm may, among other things, include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.[616]

Significant means noteworthy, important, and consequential.[617]

When assessing whether there is a "real risk of significant harm", the local authority can consider the following factors:

- Who obtained or could have obtained access to the information?
- Is there a security measure in place to prevent unauthorized access, such as encryption?
- Is the information highly sensitive?
- How long was the information exposed?
- Is there evidence of malicious intent or purpose associated with the breach, such as theft, hacking, or malware?
- Could the information be used for criminal purposes, such as for identity theft or fraud?
- Was the information recovered?
- How many individuals are affected by the breach?
- Are there vulnerable individuals involved, such as youth or seniors?[618]

For more on this topic, see the following:

---

[615] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed December 15, 2022.
[616] SK OIPC *Rules of Procedure* at p. 7.
[617] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[618] SK OIPC resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities* at p. 5, available at Privacy Breach Guidelines (oipc.sk.ca) and SK OIPC Blog: *Real Risk of Significant Harm,* January 2, 2018. Available at Real Risk of Significant Harm | IPC (oipc.sk.ca). Accessed December 16, 2022.

SK OIPC Blogs:

Real Risk of Significant Harm

Notifying affected individuals: what should I put in the letter?

SK OIPC Resources:

Privacy Breach Guidelines for Government Institutions and Local Authorities

IPC Findings

In Investigation Report 092-2022, Living Sky School Division proactively reported a breach of privacy incident to the Commissioner. The privacy breach occurred when a backpack was stolen from a privacy officer's vehicle. The backpack contained a file that had an employee's personal information in it including employment history. During the investigation by the Commissioner, it was discovered that notice of the breach was not provided by Living Sky School Division to the employee. The Commissioner determined that based on the circumstances of the case a real risk of significant harm to the employee existed and as such, Living Sky School Division should provide notice of the breach to the employee within 30 days of the issuance of the Commissioner's Report.

Privacy Breaches

A privacy breach occurs where there is an unauthorized collection, use and/or disclosure of personal information. There are also other ways a privacy breach can occur. The following is a summary of some of the causes:

Collection: A privacy breach could occur if a local authority collects personal information without authority under LA FOIP. The rules for collection are found in sections 24 and 25 of LA FOIP. Non-compliance with these sections is considered a breach of privacy.

Use: A privacy breach could occur when personal information, already in the possession or control of the local authority, is used without authority under LA FOIP. The rules for use are found in section 27 of LA FOIP. Non-compliance with this section is considered a breach of privacy.

Disclosure: A privacy breach occurs when an unauthorized disclosure of personal information transpires (e.g., when personal information is missing or when a local authority shares personal information with another organization without authority).

> Note: if personal information in the possession or control of a local authority is missing, even if there is no evidence that someone has viewed the personal information, it qualifies as a disclosure.

The rules for disclosure are found in sections 28 and 29 of LA FOIP and sections 10, 10.1 and 10.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations*.

Accuracy: Local authorities have a duty to ensure personal information is as accurate and complete as possible. A privacy breach may occur when personal information is inaccurate (see section 26 of LA FOIP).

Other sub-issues: Other issues that might arise during a privacy breach investigation could include failure to abide by the need-to-know and data minimization principles, and consent not received or issues with the form of consent. However, they would likely be tied to one of the other major issues.[619]

Privacy breaches can be very costly for organizations. The average total cost of data breach incidents for companies in Canada in 2016 was $6.03 million.[620] The cost on average per lost or stolen record was $278.[621] Privacy breaches can be costly for the organization and for affected individuals.

LA FOIP includes an explicit duty on a local authority to protect personal information in its possession or control. See *Section 23.1* earlier in this Chapter. There are also limits on collection, use and/or disclosure of personal information which helps protect the privacy of an individual's personal information. For example, by only collecting what is necessary and legitimate, a local authority avoids over-collecting personal information that could ultimately be vulnerable to a breach. See *Section 23*, *Section 24*, *Section 27*, and *Section 28*, earlier in this Chapter.

---

[619] SK OIPC resource, Privacy Breach Guidelines for Government Institutions and Local Authorities at pp. 1 to 2. Available at Privacy Breach Guidelines (oipc.sk.ca). Accessed December 16, 2022.
[620] IBM and Ponemon Institute Research Report, *2016 Cost of Data Breach Study: Canada* at p. 1. Number is based on 24 participating companies in the study.
[621] IBM and Ponemon Institute Research Report, *2016 Cost of Data Breach Study: Canada* at p. 1. Number is based on 24 participating companies in the study.

Despite every effort, privacy breaches may still occur. The following are the recommended steps to take when a local authority discovers a breach of privacy has occurred. These best practice steps and additional detail can be found in OIPC resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

Best Practice Steps for Breaches

If you have discovered a privacy breach at your organization, contact your organization's Privacy Officer immediately. Record all pertinent information related to the discovery of the breach.

If the Commissioner becomes involved, the focus will be on whether the local authority handled the breach sufficiently in accordance with the four best practice steps outlined in this section. If the Commissioner issues an Investigation Report, it will address each of these four best practice steps outlined below and how the local authority addressed each step. For more on the Commissioner's procedures when investigating a privacy breach see, *The Rules of Procedure* at Part 4.

If you have been tasked with dealing with the privacy breach, consider the following four best practice steps:

- Contain the breach
- Notify affected individuals.
- Investigate the breach.
- Prevent future breaches.

Contain the breach

It is important to contain the breach immediately. In other words, ensure that personal information is no longer at risk. This may involve:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.
- Revoking access to personal information.
- Correcting weaknesses in physical security.

Notify

The following is a list of individuals or organizations that may need to be notified as soon as possible after learning of the incident:

- Your organization's privacy officer
- The IPC (for more information see *Process for Proactively Reported* Breaches, later in this Chapter)
- The police, if criminal activity is suspected (e.g., burglary)
- The affected individuals (unless there are compelling reasons why this should not occur)

It is important to note that LA FOIP requires that, if there is an unauthorized use or disclosure of personal information, the local authority must notify the affected individual if the incident creates a "real risk of significant harm" to the affected individual (see *Section 28.1*, earlier in this Chapter).

Notification of individuals affected by the breach should occur as soon as possible after key facts about the breach have been established.

It is best to contact affected individuals directly, such as by telephone, letter or in person. However, there may be circumstances where it is not possible, and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices, media advisories and advertisements. Ensure the breach is not compounded when using indirect notification.

Notifications to affected individuals should include the following:

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may come to the affected individual because of the privacy breach.
- Steps taken and planned to mitigate the harm and prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).

- Contact information of an individual within the organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

Investigate

Once a breach has been contained the next step is to investigate the breach.

An **investigation** is a methodical process of examination, inquiry, and observation including interviewing witnesses and reviewing documents.[622]

Here are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach.
    - Has the privacy breach been contained.
    - What efforts has your organization made to contain the breach.
- What occurred
    - What type of breach occurred (e.g., collection, use, disclosure, accuracy, etc.).
    - What personal information was involved in the privacy breach.
    - When did the privacy breach occur? What are the timelines.
    - Where did the privacy breach occur.
- How did the privacy breach occur.
    - Who was involved.
    - What employees, if any, were involved with the privacy breach,. What privacy training have they received.
    - Who witnessed the privacy breach.
    - What factors or circumstances contributed to the privacy breach.
    - What is the root cause of the breach.

---

[622] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

- What is the applicable legislation and what specific sections are engaged.
- What safeguards, policies, and procedures were in place at the time of the privacy breach.
- Was the duty to protect met.
    - Were the safeguards, policies, and procedures followed.
    - If no safeguards, policies, or procedures were in place, why not.
    - Were the individuals involved aware of the safeguards, policies, and procedures.
- Who are the affected individuals.
    - How many are there.
    - What are the risks associated to a privacy breach involving this information (e.g., is the affected individual at risk for identity theft, credit card fraud, etc.).
    - Have affected individuals been notified of the privacy breach.

Once the necessary information has been collected, it is a good idea to prepare an internal privacy breach investigation report. The report should include the following:

- Summary of the incident and immediate steps taken to contain the breach.
- Background of the incident, timelines, and a chronology of events.
- Description of the personal information involved and affected individuals.
- Description of the investigative process.
- The root and contributing causes of the incident.
- A review of applicable legislation, safeguards, policies, and procedures.
- Summary of possible solutions and recommendations for preventing future breaches. This should include specific timelines and responsibility for implementation of each action.

During an investigation by the IPC (or when proactively reporting a privacy breach to the IPC – see below for more), the IPC will also request that local authorities complete the IPC's *Privacy Breach Investigation Questionnaire*.

Conducting Root Cause Analysis[623]

Root Cause Analysis is a useful process for understanding and solving a problem. It seeks to identify the origin of a problem by using a specific set of steps and tools to:

- Determine what happened.
- Determine why it happened.
- Figure out what to do to reduce the likelihood that it will happen again.

You can apply Root Cause Analysis to almost any situation. Determining how far to go in your investigation requires good judgement and common sense. It is important to recognize when a significant cause that can be changed is identified.

Follow the steps and use the template when you want to conduct a comprehensive review of a significant problem and identify the events and factors that led to the root cause.

Root Cause Analysis assumes that systems and events are interrelated; an action in one area often triggers an action in another. By tracing back these actions, you can discover where the problem started and how it grew into the symptom now being faced.

There are three basis causes:

i. **Physical causes** – something failed in some way (e.g., a car's brakes stopped working).

ii. **Human causes** – people did something wrong or did not do something that was needed. Human causes typically lead to physical causes (e.g., no one filled the brake fluid, which led to the brakes failing).

iii. **Organizational causes** – a system, process or policy that people use to make decisions (e.g., no one person was responsible for vehicle maintenance, and everyone assumed someone else had filled the brake fluid).

---

[623] This section reproduced from Keith, Lori D., Pealow, James B., *First Nations Health Managers: Human Resources, Programs and Support Services Toolbox*, 2012. Ottawa: First Nations Health Managers Association at pp. 52 to 53.

Root Cause Analysis looks at all three types of causes. It involves investigating the patterns of negative effects, finding hidden flaws in the system, and discovering specific actions that contributed to the problem. This often means the Root Cause Analysis reveals more than one root case.

Five Steps to Conduct a Root Cause Analysis

1. **Define the Problem**
    a. What do you see happening.
    b. What are the specific symptoms.

2. **Collect Data**
    a. What proof do you have that the problem exists.
    b. How long has the problem existed.
    c. What is the impact of the problem.

You need to fully analyze a situation before you can look at factors that contributed to the problem. To maximize the effectiveness of your Root Cause Analysis, get everyone together who understands the situation. People who are most familiar with the problem can help lead you to a better understanding of the issues.

A helpful approach is to look at the same situation from different perspectives; the clients, the staff who implement the solutions, the community and the leadership.

3. **Identify Possible Causal Factors**
    a. What sequence of events led to the problem.
    b. What conditions allow the problem to occur.
    c. What other problems surround the occurrence of the central problem.

During this stage, identify as many causal factors as possible. With Root Cause Analysis, you do not want to simply treat the most obvious causes – you want to dig deeper.

Some tools that help identify causal factors are:

- *Appreciative Inquiry* – Use the facts and ask, "So what?" to determine all the possible consequences of a fact.
- *Five Whys* – Ask "Why?" until you get to the root of the problem. The 'Five Whys' is a method for rapidly determining the root cause of a problem. It involves asking 'why'

until you reach the real source of the problem. Asking 'why' five times usually gathers the right information to fix the problem.

Example:

Problem: People are falling more often in our department.

1) *Why?* The floors are slippery.

2) *Why?* The cleaners are using a new cleaning product.

3) *Why?* The suppliers offered a special deal on a new product.

4) *Why?* To save money on cleaning supplies.

5) *Why?* The buying process has no standardized process that considers the risks and benefits of trying new products.

- *Drill Down* – Break down a problem into small, detailed parts to better understand the big picture.
- *Cause and Effect Diagrams* – Create a chart of all the possible causal factors to identify where the trouble may have begun.

4. Identify the Root Cause(s)

a. Why does the causal factor exist.
b. What is the real reason the problem occurred.

Use the same tools you used to identify the causal factors (in Step 3) to look at the roots of each factor. These tools are designed to encourage you to dig deeper at each level of cause and effect.

5. Recommend and Implement Solutions

a. What can you do to prevent the problem from happening again.
b. How will the solution be implemented.
c. Who will be responsible for it.
d. What are the risks of implementing the solution.

Analyze your cause-and-effect process and identify the changes that are needed. It is also important that you plan ahead to predict the effects of your solution. This way, you can spot potential failures before they happen.

Prevent

The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring.

- What steps can be taken to prevent a similar privacy breach.
    - Can your organization create or make changes to policies and procedures relevant to this privacy breach.
    - Are additional safeguards needed.
    - Is additional training needed.
    - Should a practice be stopped.

How IPC Investigations are Initiated

The IPC can learn of a privacy breach and begin an investigation in several different ways. Some of them include:

- A citizen comes to the IPC with a complaint about a local authority's actions or practices.
- A third party in possession of personal information could notify the IPC.
- Employees of a local authority inform the IPC of inappropriate practices within the organization.
- The IPC acts on media reports.
- The local authority proactively reports a breach to the IPC. The next section details the process when a local authority proactively reports a breach to the IPC.

Process for Proactively Reported Breaches

Local authorities should consider proactively reporting privacy breaches to the IPC. This means that when a local authority learns of a breach, it reports it to the IPC. While not mandatory, the IPC does encourage local authorities to proactively report.

To assist local authorities, the IPC has developed a reporting form to proactively report a privacy breach to the IPC:

> *Proactively Reported Breach of Privacy Reporting Form for Public Bodies*.

Local authorities should complete this form and submit it to intake@oipc.sk.ca.

Advantages of proactively reporting of proactively reporting include:

- May reduce the need for the IPC to issue a public report on the matter.
- Receive timely, expert advice from the IPC - the IPC can help guide the local authority on what to consider, what questions to ask, and what parts of LA FOIP or *The Local Authority Freedom of Information and Protection of Privacy Regulations* may be applicable.
- Should the media contact the local authority, the local authority can advise it has notified the IPC of the privacy breach and will seek assistance from the IPC with handling it.
- Should affected individuals contact the IPC, the IPC can assure the individuals that the IPC is aware of the breach which may prevent a formal complaint to the IPC.

When a local authority proactively reports a privacy breach to the IPC, a file will be opened.

The local authority will be asked to complete and provide the IPC's *Privacy Breach Investigation Questionnaire* (Questionnaire) and any other relevant material within 30 days.

The Questionnaire takes local authorities through the four best practice steps of responding to a breach (containment, notification, investigation and prevention of future breaches). The completed Questionnaire should provide the IPC with what is required to conduct an investigation. If further information is required, the IPC will advise.

Once the IPC receives the relevant material, it will review the file and make a decision. The possible outcomes are as follows:

- If the Commissioner is satisfied with the local authority's overall response to the breach, the file will be closed informally without a public report. This process may include some informal recommendations from the IPC.
- If the breach is egregious or it involves a large number of affected individuals, the Commissioner may determine that a report will be issued.

- If an affected individual makes a formal complaint, the Commissioner may determine that a report will be issued.
- If the Commissioner is not satisfied with the local authority's response or handling of the breach, the IPC will issue a report.

Once the IPC has made a decision, the local authority will be advised if a report will be issued or not. The local authority will also be notified if an affected individual makes a formal complaint, which may also result in a public report.[624]

If you have questions or need further guidance, contact the SK OIPC at intake@oipc.sk.ca.

Section 29: Personal information of deceased individual

Personal information of deceased individual

29(1) Subject to subsection (2) and to any other Act, the personal information of a deceased individual shall not be disclosed until 25 years after the death of the individual.

(2) Where, in the opinion of the head, disclosure of the personal information of a deceased individual to the individual's next of kin would not constitute an unreasonable invasion of privacy, the head may disclose that personal information before 25 years have elapsed after the individual's death.

Subsection 29(1)

Personal information of deceased individual

29(1) Subject to subsection (2) and to any other Act, the personal information of a deceased individual shall not be disclosed until 25 years after the death of the individual.

Subsection 29(1) of LA FOIP provides that the personal information of a deceased individual cannot be disclosed until 25 years after the death of the individual.

This provision puts a time limit on the protection of privacy after death. LA FOIP protects the privacy rights of an individual who has been dead less than 25 years, with certain exceptions.

---

[624] For more, see SK OIPC resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities.* Available at Privacy Breach Guidelines (oipc.sk.ca).

Once an individual has been dead 25 years or more, release of his or her personal information is permitted, and it is no longer subject to the privacy protections under LA FOIP. The provision is particularly important for permitting historical and genealogical research.[625]

When considering disclosure under this provision, local authorities should be confident in how long the individual has been deceased. If an applicant is requested access under LA FOIP to a deceased individual's personal information, the applicant should be able to provide evidence, such as a death certificate, that an individual has been dead for 25 years or more.[626]

When considering the application of this provision, local authorities should also consider whether section 49 of LA FOIP (exercise of rights by other persons) has any application in the circumstances.

In some instances, *personal representatives* may be exercising a right or power as it relates to the administration of the individual's estate. Further, there may be written authorization from the individual prior to death (see subsection 49(e) of LA FOIP).

For more on section 49, see *Guide to LA FOIP*, Chapter 3: "Access to Records", *Exercise of Rights by Authorized Representatives*.[627]

IPC Findings

In Investigation Report 282-2018, the Commissioner investigated an alleged breach of privacy involving the Rural Municipality of Parkdale (RM). The complaint alleged that the RM posted personal information of a deceased employee in its council meeting minutes which were then posted on the RM's website. The RM asserted it had authority to disclose the personal information pursuant to subsection 29(2) of LA FOIP. Although the RM did not make a persuasive argument as to how the provision applied, the Commissioner noted that the RM appeared to be relying on the provision because the surviving spouse of the employee publicly shared some of the deceased employee's personal information first. However, this was not persuasive. The Commissioner found that the RM did not share the personal information with next of kin as required by subsection 29(2) of LA FOIP and therefore the RM could not rely on subsection 29(2) of LA FOIP for the disclosure.

[625] Adapted from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 120.
[626] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 120.
[627] Also see section 49 (Exercise of rights by other persons) in LA FOIP.

In Investigation Report 041-2017, the Commissioner investigated an alleged breach of privacy involving the former Prince Albert Parkland Regional Health Authority (Parkland). The Prince Albert Historical Society reported to the Commissioner that it received a filing cabinet from Parkland that contained the records of nursing students who were graduates of Holy Family School of Nursing from 1910 to 1969. The Commissioner determined that Parkland had control over these records and was therefore responsible for their disposition. The Commissioner recommended that Parkland integrate the records into its records management system. Further, as some records were over 100 years old there would be authority to the disclose those records pursuant to subsection 29(1) of LA FOIP. In addition, if former students were deceased, Parkland could disclose the records to family members if the students had been deceased less than 25 years pursuant to subsection 29(2) of LA FOIP.

Subsection 29(2)

Personal information of deceased individual

29(2) Where, in the opinion of the head, disclosure of the personal information of a deceased individual to the individual's next of kin would not constitute an unreasonable invasion of privacy, the head may disclose that personal information before 25 years have elapsed after the individual's death.

Subsection 29(2) of LA FOIP gives the head discretion to disclose the personal information of a deceased individual before 25 years after death to the individual's next of kin where it is deemed not to constitute an unreasonable invasion of privacy.

Next of kin is a person's nearest relative by blood or marriage which could include a cousin, grandparent, niece or nephew, who has close ties to the individual who is deceased. For example:

- Spouse, parent, child.
- Cousins brought up together as siblings.
- A grandchild brought up by grandparents.[628]

[628] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Unreasonable means going beyond the limits of what is reasonable or equitable.[629]

Invasion of privacy is a term that means the privacy of a person has been invaded.[630] *Invasion* means an encroachment upon the rights of another.[631] An encroachment on the privacy rights under Part IV of LA FOIP which pertains to the collection, use and/or disclosure of one's personal information under LA FOIP.

When considering this provision, the "invasion-of-privacy" test can assist to determine the level of privacy risk in the disclosure. It involves a detailed review of three interrelated risk factors that may help determine whether disclosure poses an unreasonable invasion of privacy. These three factors are the sensitivity of the information, the expectations of the individual and the probability and degree of injury. In addition, local authorities should consider factors unique to their own operational context, as applicable.[632] For example, for purposes of subsection 29(2) of LA FOIP, a consideration would be how long the individual has been deceased. Deceased individuals have privacy rights, but they diminish over time.[633] Other relevant motives could be the reason an applicant seeks access. The motive of an applicant is not usually relevant in access requests, however, in the context of cases involving family members seeking information to deal with a death and its aftermaths, it has been considered appropriate to do so.[634]

(1) Sensitivity of the information

- Consider whether the type of information is of a detailed (e.g., name and address) or highly personal (e.g., health information) nature.
- Evaluate the context in which the information was collected and determine whether any contextual sensitivities apply to the information. For example, a list of public servants may not be considered particularly sensitive, but that

---

[629] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-238. Available at Chapter (gov.mb.ca). Accessed December 16, 2022.
[630] The Law Dictionary, Black's Law Dictionary, Free 2nd ed. Available at INVASION OF PRIVACY Definition & Meaning - Black's Law Dictionary (thelawdictionary.org).
[631] The Law Dictionary, Black's Law Dictionary, Free 2nd ed. Available at INVASION Definition & Meaning - Black's Law Dictionary (thelawdictionary.org).
[632] Adapted from Privacy Commissioner of Canada, *Public Interest Disclosures by federal institutions under the Privacy Act*, revised June 2022. Available at Public interest disclosures by federal institutions under the Privacy Act - Office of the Privacy Commissioner of Canada. Accessed December 15, 2022.
[633] BC IPC Order F15-36 at [29]. At paragraphs [29] to [30] of this Order, the BC IPC established that 2 ½ years or less since the individual died was not a sufficient amount of time to justify release on that factor alone.
[634] BC IPC Order F15-36 at [31]. At paragraphs [29].

same list, if collected to identify employees having a specific illness would be considered sensitive based on the context.

(2) Expectations of the individual

- Evaluate the conditions under which the personal information was collected and consider what expectations the collecting institution may have established for its confidentiality, including whether the possibility of disclosure is conveyed in an applicable Privacy Notice Statement.
- Consider the reasonable expectations of privacy that apply to the context in which the information was collected. To determine what constitutes a reasonable expectation of privacy, courts will look at the totality of circumstances. This could include location of collection (e.g., in a private conversation as compared to a public town hall), context of collection (e.g., in a routine application for services as compared to a letter sent to several local authorities), etc.

(3) Probability and degree of injury

- Consider the probability and degree or gravity of injury relative to the benefits of the disclosure to the public. This could include personal or physical injury, or damage to the reputation of an individual or others, which causes adverse consequences (e.g., any harm or embarrassment that negatively affects an individual's career, reputation, financial position, safety, health or well-being).
- Determine the potential of injury if the receiving party wrongfully disclosed the information further.[635]

Local authorities should still abide by the data minimization and need-to-know principles when disclosing personal information. Only disclose the least amount of personal information necessary to achieve the purpose. Further, only disclose to those that have a need-to-know the personal information to carry out the purpose. See *Need-to-Know* and *Data Minimization* earlier in this Chapter.

[635] Privacy Commissioner of Canada, *Public Interest Disclosures by federal institutions under the Privacy Act*, revised June 2022. Available at Public interest disclosures by federal institutions under the Privacy Act - Office of the Privacy Commissioner of Canada. Accessed December 15, 2022.

IPC Findings

In Investigation Report 282-2018, the Commissioner investigated an alleged breach of privacy involving the Rural Municipality of Parkdale (RM). The complaint alleged that the RM posted personal information of a deceased employee in its council meeting minutes which were then posted on the RM's website. The RM asserted it had authority to disclose the personal information pursuant to subsection 29(2) of LA FOIP. Although the RM did not make a persuasive argument as to how the provision applied, the Commissioner noted that the RM appeared to be relying on the provision because the surviving spouse of the employee publicly shared some of the deceased employee's personal information first. However, this was not persuasive. The Commissioner found that the RM did not share the personal information with next of kin as required by subsection 29(2) of LA FOIP and therefore the RM could not rely on subsection 29(2) of LA FOIP for the disclosure.

In Investigation Report 041-2017, the Commissioner investigated an alleged breach of privacy involving the former Prince Albert Parkland Regional Health Authority (Parkland). The Prince Albert Historical Society reported to the Commissioner that it received a filing cabinet from Parkland that contained the records of nursing students who were graduates of Holy Family School of Nursing from 1910 to 1969. The Commissioner determined that Parkland had control over these records and was therefore responsible for their disposition. The Commissioner recommended that Parkland integrate the records into its records management system. Further, as some records were over 100 years old there would be authority to the disclose those records pursuant to subsection 29(1) of LA FOIP. In addition, if former students were deceased, Parkland could disclose the records to family members if the students had been deceased less than 25 years pursuant to subsection 29(2) of LA FOIP.

Section 30: Access to personal information

Individual's access to personal information

30(1) Subject to Part III and subsections (2) and (3), an individual whose personal information is contained in a record in the possession or under the control of a local authority has a right to, and:

(a) on an application made in accordance with Part II; and

(b) on giving sufficient proof of his or her identity;

shall be given access to the record.

(2) A head may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of determining the individual's suitability, eligibility or qualifications for employment or for the awarding of government contracts and other benefits by the local authority, where the information is provided explicitly or implicitly in confidence.

(3) The head of the University of Saskatchewan or the University of Regina may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of:

(a) determining the individual's suitability for:

(i) appointment, promotion or tenure as a member of the faculty of the University of Saskatchewan or the University of Regina;

(ii) admission to an academic program; or

(iii) receipt of an honour or aware; or

(b) evaluating the individual's research projects or materials for publication;

where the information is provided explicitly or implicitly in confidence.

This section can also be found in the *Guide to LA FOIP*, Chapter 3: "Access to Information" and Chapter 4: "Exemptions to the Right of Access". It is reproduced here for ease of access and because it falls under Part IV of LA FOIP which deals with "personal information".

Subsection 30(1)

Individual's access to personal information

30(1) Subject to Part III and subsections (2) and (3), an individual whose personal information is contained in a record in the possession or under the control of a local authority has a right to, and:

(a) on an application made in accordance with Part II; and

(b) on giving sufficient proof of his or her identity;

shall be given access to the record.

Subsection 30(1) of LA FOIP provides that upon application an individual is entitled to their own personal information contained within a record unless an exemption applies under Part III or subsections 30(2) and (3) of LA FOIP applies.

Local authorities should interpret the exemptions to this right to personal information with a view to giving an individual as much access as possible.

Records containing personal information may be very sensitive in nature, so care must be taken to ensure that proper safeguards are in place when these types of records are released. When providing an applicant with access to personal information, a local authority must be satisfied that the individual receiving the information is indeed the individual that the information is about or a duly appointed representative of that person.21[636] For more on duly appointed representatives, see *Guide to LA FOIP*, Chapter 3: "Access to Information", *Section 49: Exercise of Rights by Other Persons*.[637]

For more information on verifying the identity of the applicant, the Ministry of Justice, Access and Privacy Branch issued the resource, *Verifying the Identity of an Applicant*. It provides helpful direction on steps that can be taken to verify identity.

Subsection 30(2)

Individual's access to personal information

30(2) A head may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of determining the individual's suitability, eligibility or qualifications for employment or for the awarding of contracts and other benefits by the local authority, where the information is provided explicitly or implicitly in confidence.

Subsection 30(2) of LA FOIP enables the head to refuse to disclose to individuals, personal information that is evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility or qualifications for employment or for the awarding of contracts and other benefits by the local authority.

The provision attempts to address two competing interests: the right of an individual to have access to his or her personal information and the need to protect the flow of frank

[636] Government of Saskatchewan, Ministry of Justice, Access and Privacy Branch, Resource, *Verifying the Identity of an Applicant*, September 2017, at p. 2.
[637] See also section 49 in LA FOIP.

information to local authorities so that appropriate decisions can be made respecting the awarding of jobs, contracts, and other benefits.[638]

The following three-part test can be applied:

1. Is the information personal information that is evaluative or opinion material?

To qualify as *personal information*, the information must be about an identifiable individual and must be personal in nature. Some examples are provided in subsection 23(1) of LA FOIP. See *Section 23* earlier in this Chapter.

Evaluative means to have assessed, appraised, to have found or to have stated the number of.[639]

Opinion material is a belief or assessment based on grounds short of proof; a view held as probable for example, a belief that a person would be a suitable employee, based on that person's employment history. An opinion is subjective in nature and may or may not be based on facts.[640]

2. Was the personal information compiled solely for one of the enumerated purposes?

Compiled means that the information was drawn from several sources or extracted, extrapolated, calculated or in some other way manipulated.[641]

The enumerated purposes are:

- For determining the individual's suitability, eligibility, or qualifications for employment.
- For the awarding of contracts with the local authority.
- For awarding other benefits by the local authority.

---

[638] Adapted from ON IPC Order P-773. Ontario has a similar provision at subsection 49(c) of its *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31.
[639] AB IPC Order 98-021 at p.4.
[640] AB IPC Order 98-021 at p.4.
[641] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.

Suitability means right or appropriate for a particular person, purpose, or situation.[642]

Eligibility means fit and proper to be selected or to receive a benefit; legally qualified for an office, privilege, or status.[643]

Qualifications means the possession of qualities or properties inherently or legally necessary to make one eligible for apposition or office, or to perform a public duty or function.[644]

Employment means the selection for a position as an employee of a local authority.[645]

Employment reference means personal information that is evaluative, or opinion material compiled solely for the purpose of describing an individual's suitability, eligibility, or qualifications for employment.[646]

Award means to give or to order to be given as a payment, compensation, or prize; to grant; to assign.[647]

Benefit means a favourable or helpful factor or circumstance; advantage, profit.[648]

Other benefits refer to benefits conferred by a local authority through an evaluative process. The term includes research grants, scholarships, and prizes. It also includes appointments required for employment in a particular job or profession such as a bailiff or special constable.[649]

Employee of a local authority means an individual employed by a local authority and includes an individual retained under a contract to perform services for the local authority.[650]

---

[642] Pearsall, Judy, *Concise Oxford Dictionary, 10th Ed.*, (Oxford University Press) at p. 1434.
[643] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 657.
[644] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1497.
[645] Service Alberta, *FOIP Guidelines and Practices, 2009 Edition*, Chapter 4 at p. 141.
[646] *The Local Authority Freedom of Information and Protection of Privacy Regulations,* c. L-27.1 Reg. 1, s. 2(1)(b).
[647] AB IPC, Order 98-021 at p.5.
[648] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[649] Service Alberta, *FOIP Guidelines and Practices, 2009 Edition*, Chapter 4 at p. 141.
[650] *The Local Authority Freedom of Information and Protection of Privacy Act* [S.S. 1990-91, c L-27.1], s. 2(b.1).

The personal information must have been compiled solely for one of the enumerated purposes to qualify.

3. Was the personal information provided explicitly or implicitly in confidence?

In confidence usually describes a situation of mutual trust in which private matters are relayed or reported. Information provided *in confidence* means that the supplier of the information has stipulated how the information can be disseminated.[651] In order for confidence to be found, there must be an implicit or explicit agreement or understanding of confidentiality on the part of both the local authority and the party providing the information.[652]

Implicitly means that the confidentiality is understood even though there is no actual statement of confidentiality, agreement, or other physical evidence of the understanding that the information will be kept confidential.[653]

Explicitly means that the request for confidentiality has been clearly expressed, distinctly stated, or made definite. There may be documentary evidence that shows that the information was provided on the understanding that it would be kept confidential.[654]

Factors considered when determining whether a document was provided in confidence *implicitly* include (not exhaustive):

- What is the nature of the information. Would a reasonable person regard it as confidential. Would it ordinarily be kept confidential by the party providing it or by the local authority.[655]
- Was the information treated consistently in a manner that indicated a concern for its protection by the party providing it and the local authority from the point at which it was provided until the present time.[656]

---

[651] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 104, SK OIPC Review Reports F-2006-002 at [51], H-2008-002 at [73], ON IPC Order MO-1896 at p. 8.
[652] SK OIPC Review Reports F-2006-002 at [52], LA-2013-002 at [57]; ON IPC Order MO-1896 at p. 8.
[653] SK OIPC Review Reports F-2006-002 at [57], F-2009-001 at [62], F-2012-001/LA-2012-001 at [29], LA-2013-002 at [49], F-2014-002 at [47].
[654] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at pp. 104 and 105.
[655] BC IPC Orders 331-1999 at [8], F13-01 at [23]; NS IPC Review Reports 17-03 at [34], 16-09 at [44]; PEI IPC Order FI-16-006 at [19].
[656] ON IPC Orders PO-2273 at p. 8, PO-2283 at p. 10.

- Is the information available from sources to which the public has access.[657]
- Does the local authority have any internal policies or procedures that speak to how records or information such as that in question are to be handled confidentially.
- Was there a mutual understanding that the information would be held in confidence. **Mutual understanding** means that the local authority and the party providing it both had the same understanding regarding the confidentiality of the information at the time it was provided. If one party intended the information to be kept confidential but the other did not, the information is not considered to have been provided in confidence. However, mutual understanding alone is not sufficient. Additional factors must exist.[658]

The preceding factors are not a test but rather guidance on factors to consider. It is not an exhaustive list. Each case will require different supporting arguments. The bare assertion that the information was provided implicitly in confidence would not be sufficient.[659]

Factors to consider when determining if a document was provided in confidence *explicitly* include (not exhaustive):

- The existence of an express condition of confidentiality between the local authority and the party providing it.[660]
- The fact that the local authority requested the information be provided in a sealed envelope and/or outlined its confidentiality intentions to the party prior to the information being provided.[661]

The preceding factors are not a test but rather guidance on factors to consider. It is not an exhaustive list. Each case will require different supporting arguments.

Two cases came before the Court of King's Bench for Saskatchewan dealing with subsection 30(2) of LA FOIP. Those two cases are as follows:

---

[657] ON IPC Orders PO-2273 at p. 8, PO-2283 at p. 10.
[658] *Jacques Whitford Environment Ltd. v. Canada (Minister of National Defence)*, 2001 FCT 556 at [40]; SK OIPC Review Reports F-2006-002 at [52], LA-2013-002 at [58] to [59]; ON IPC Order MO-1896 at p. 8; BC IPC Order F-11-08 at [32].
[659] SK OIPC Review Report LA-2013-002 at [60].
[660] SK OIPC Review Reports F-2006-002 at [56], LA-2013-003 at [113], F-2014-002 at [47]; PEI IPC Order 03-006 at p. 5; AB IPC Orders 97-013 at [23] to [24], 2001-008 at [54].
[661] SK OIPC Review Reports F-2006-002 at [56], F-2012-001/LA-2012-001 at [29], LA-2013-002 at [49], LA-2013-003 at [113], F-2014-002 at [47]; PEI IPC Order 03-006 at p. 5; AB IPC Order 97-013 at [25].

- *Fogal v. Regina School Division No. 4*, 2002 SKKB 92 (CanLII)
- *Britto v University of Saskatchewan*, 2018 SKKB 92 (CanLII)

IPC Findings

In Review Report LA-2004-001, the Commissioner reviewed a denial of access by the Lloydminster Public School Division (Division). An applicant requested access to records related to the applicant's suitability for volunteering in after-school sport activities. Upon review, the Commissioner found that the evaluative or opinion material was not compiled for the purpose of determining the applicant's suitability, eligibility or qualifications for employment or for the awarding of a contract or other benefit. It was compiled for the purpose of determining the suitability of a volunteer to engage in "volunteer" activity in an after-hours sports program. The Commissioner found that a volunteer does not meet the definition of "employee" of a local authority. As such, the Commissioner found that subsection 30(2) of LA FOIP did not apply.

In Review Report 258-2016, the Commissioner found that the name of the individual giving the opinion was also captured by the provision. The purpose and intent of the provision is to allow individuals to provide frank feedback where there is an evaluation process occurring. In addition, evaluating suitability for employment can take place not only during the hiring process but also during an employee's tenure. Further, the provision can include unsolicited records such as letters of concern or complaint (*Fogal v. Regina School Division No. 4, (2002)*).

In Review Report 010-2018, the Commissioner reviewed a denial of access by the South East Cornerstone Public School Division #209 (Cornerstone). An applicant was seeking parental complaints and witness statements regarding an incident. Cornerstone withheld the records pursuant to several provisions in LA FOIP including subsection 30(2) of LA FOIP. Upon review, the Commissioner found that the records contained personal information that was evaluative or opinion material. Further, the Commissioner found that the personal information was compiled solely for the purpose of determining the applicant's suitability for employment. Finally, the Commissioner found that the interview notes were provided explicitly in confidence. However, the written complaints were not provided implicitly or explicitly in confidence. The Commissioner recommended that Cornerstone sever the opinions and other personal information of individuals other than the applicant and release the rest.

In Review Report 142-2022, the Commissioner considered a denial of access involving the Ministry of Social Services (Social Services). Social Services withheld portions of the record totaling 255 pages. It applied the equivalent subsection 31(2) of *The Freedom of Information and Protection of Privacy Act* (FOIP) to portions of the records. Upon review, the

Commissioner found that the assessment information collected on the applicant was for the enumerated purpose of determining eligibility to an income program offered by Social Services. The assessment information contained the comments of the assessor. However, the Commissioner found that Social Services did not demonstrate that the scores on the assessment were provided explicitly or implicitly in confidence. As such, the Commissioner found that subsection 31(2) of FOIP did not apply.

Subsection 30(3)

Individual's access to personal information

30(3) The head of the University of Saskatchewan or the University of Regina may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of:

(a) determining the individual's suitability for:

(i) appointment, promotion or tenure as a member of the faculty of the University of Saskatchewan or the University of Regina;

(ii) admission to an academic program; or

(iii) receipt of an honour or award; or

(b) evaluating the individual's research projects or materials for publication;

where the information is provided explicitly or implicitly in confidence.

Subsection 30(3) of LA FOIP provides that the head of the University of Saskatchewan or the University of Regina may refuse to disclose an individual's personal information in certain circumstances.

Subsection 30(3)(a)

Individual's access to personal information

30(3) The head of the University of Saskatchewan or the University of Regina may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of:

(a) determining the individual's suitability for:

(i) appointment, promotion or tenure as a member of the faculty of the University of Saskatchewan or the University of Regina;

(ii) admission to an academic program; or

(iii) receipt of an honour or award; or

…

where the information is provided explicitly or implicitly in confidence.

Subsection 30(3)(a) of LA FOIP provides the University of Saskatchewan and University of Regina ability to withhold personal information if it is evaluative or opinion material compiled for the purposes of:

- determining the individual's suitability for:
    - an appointment, promotion, tenure as a member of the faculty;
    - admission to an academic program; or
    - for the receipt of an honour or award;

  where the information was provided explicitly or implicitly in confidence.

The following three-part test can be applied:

1. Is the information personal information that is evaluative or opinion material?

To qualify as *personal information*, the information must be about an identifiable individual and must be personal in nature. Some examples are provided in subsection 23(1) of LA FOIP. See *Section* 23 earlier in this Chapter for more explanation on what constitutes personal information.

Evaluative means to have assessed, appraised, to have found or to have stated the number of.[662]

Opinion material is a belief or assessment based on grounds short of proof; a view held as probable for example, a belief that a person would be a suitable employee, based on that person's employment history. An opinion is subjective in nature and may or may not be based on facts.[663]

2. Was the personal information compiled solely for one of the enumerated purposes?

Compiled means that the information was drawn from several sources or extracted, extrapolated, calculated or in some other way manipulated.[664]

The enumerated purposes are:

- determining the individual's suitability for appointment, promotion, or tenure as a member of the faculty; or
- for determining the individual's suitability for admission to an academic program; or
- for determining the individual's suitability to receive an honour or award.

The personal information must have been compiled solely for one of the enumerated purposes to qualify.

Award means to give or to order to be given as a payment, compensation, or prize; to grant; to assign. In this context, it implies that the decision-maker has some authority to give or to order that benefit be granted.[665]

3. Was the personal information provided explicitly or implicitly in confidence?

In confidence usually describes a situation of mutual trust in which private matters are relayed or reported. Information provided *in confidence* means that the supplier of the

---

[662] AB IPC Order 98-021 at p.4.
[663] AB IPC Order 98-021 at p.4.
[664] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[665] AB IPC, Order 98-021 at p.5.

information has stipulated how the information can be disseminated.[666] In order for confidence to be found, there must be an implicit or explicit agreement or understanding of confidentiality on the part of both the local authority and the party providing the information.[667]

Implicitly means that the confidentiality is understood even though there is no actual statement of confidentiality, agreement, or other physical evidence of the understanding that the information will be kept confidential.[668]

Explicitly means that the request for confidentiality has been clearly expressed, distinctly stated, or made definite. There may be documentary evidence that shows that the information was provided on the understanding that it would be kept confidential.[669]

Factors considered when determining whether a document was provided in confidence *implicitly* include (not exhaustive):

- What is the nature of the information? Would a reasonable person regard it as confidential? Would it ordinarily be kept confidential by the party providing it or by the local authority?[670]
- Was the information treated consistently in a manner that indicated a concern for its protection by the party providing it and the local authority from the point at which it was provided until the present time?[671]
- Is the information available from sources to which the public has access?[672]
- Does the local authority have any internal policies or procedures that speak to how records or information such as that in question are to be handled confidentially?
- Was there a mutual understanding that the information would be held in confidence? **Mutual understanding** means that the local authority and the party providing it both had the same understanding regarding the confidentiality of the information at the time it was provided. If one party intended the information to be kept confidential but

[666] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 104, SK OIPC Review Reports F-2006-002 at [51], H-2008-002 at [73], ON IPC Order MO-1896 at p. 8.
[667] SK OIPC Review Reports F-2006-002 at [52], LA-2013-002 at [57]; ON IPC Order MO-1896 at p. 8.
[668] SK OIPC Review Reports F-2006-002 at [57], F-2009-001 at [62], F-2012-001/LA-2012-001 at [29], LA-2013-002 at [49], F-2014-002 at [47].
[669] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at pp. 104 and 105.
[670] BC IPC Orders 331-1999 at [8], F13-01 at [23]; NS IPC Review Reports 17-03 at [34], 16-09 at [44]; PEI IPC Order FI-16-006 at [19].
[671] ON IPC Orders PO-2273 at p. 8, PO-2283 at p. 10.
[672] ON IPC Orders PO-2273 at p. 8, PO-2283 at p. 10.

the other did not, the information is not considered to have been provided in confidence. However, mutual understanding alone is not sufficient. Additional factors must exist in addition.[673]

The preceding factors are not a test but rather guidance on factors to consider. It is not an exhaustive list. Each case will require different supporting arguments. The bare assertion that the information was provided implicitly in confidence would not be sufficient.[674]

Factors to consider when determining if a document was provided in confidence *explicitly* include (not exhaustive):

- the existence of an express condition of confidentiality between the local authority and the party providing it;[675]
- the fact that the local authority requested the information be provided in a sealed envelope and/or outlined its confidentiality intentions to the party prior to the information being provided.[676]

The preceding factors are not a test but rather guidance on factors to consider. It is not an exhaustive list. Each case will require different supporting arguments.

IPC Findings

In Review Report 164-2016, the Commissioner reviewed a denial of access by the University of Saskatchewan (U of S). An applicant requested access to material related to his application to medical residency programs at the U of S. The U of S withheld portions of the records citing several exemptions under LA FOIP including subsection 30(3)(a)(ii) of LA FOIP. Upon review, the Commissioner considered subsection 30(3)(a)(ii) of LA FOIP which was applied to reference letters submitted to the U of S on behalf of the applicant and scores and notes made by the individuals reviewing the applicant's applications for residency positions. The

[673] *Jacques Whitford Environment Ltd. v. Canada (Minister of National Defence)*, 2001 FCT 556 at [40]; SK OIPC Review Reports F-2006-002 at [52], LA-2013-002 at [58] to [59]; ON IPC Order MO-1896 at p. 8; BC IPC Order F-11-08 at [32].
[674] SK OIPC Review Report LA-2013-002 at [60].
[675] SK OIPC Review Reports F-2006-002 at [56], LA-2013-003 at [113], F-2014-002 at [47]; PEI IPC Order 03-006 at p. 5; AB IPC Orders 97-013 at [23] to [24], 2001-008 at [54].
[676] SK OIPC Review Reports F-2006-002 at [56], F-2012-001/LA-2012-001 at [29], LA-2013-002 at [49], LA-2013-003 at [113], F-2014-002 at [47]; PEI IPC Order 03-006 at p. 5; AB IPC Order 97-013 at [25].

Commissioner found that the three part test was met and that the U of S appropriately applied subsection 30(3)(a)(ii) of LA FOIP.

Subsection 30(3)(b)

Individual's access to personal information

30(3) The head of the University of Saskatchewan or the University of Regina may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of:

…

(b) evaluating the individual's research projects or materials for publication;

where the information is provided explicitly or implicitly in confidence.

Subsection 30(3)(b) of LA FOIP provides the U of S and U of R ability to withhold personal information if it is evaluative or opinion material compiled for the purpose of evaluating an individual's research projects or materials for publication.

The following three-part test can be applied:

1. Is the information personal information that is evaluative or opinion material?

To qualify as *personal information*, the information must be about an identifiable individual and must be personal in nature. Some examples are provided in subsection 23(1) of LA FOIP. See *Section 23* earlier in this Chapter for more explanation on what constitutes personal information.

Evaluative means to have assessed, appraised, to have found or to have stated the number of.[677]

Opinion material is a belief or assessment based on grounds short of proof; a view held as probable for example, a belief that a person would be a suitable employee, based on that person's employment history. An opinion is subjective in nature and may or may not be based on facts.[678]

[677] AB IPC Order 98-021 at p.4.
[678] AB IPC Order 98-021 at p.4.

2. Was the personal information compiled solely for the purpose of evaluating the individual's research projects or materials for publication?

Compiled means that the information was drawn from several sources or extracted, extrapolated, calculated or in some other way manipulated.[679]

The personal information must have been compiled solely for the purpose of evaluating the individual's research projects or materials for publication to qualify.

Evaluate means to form an idea of the amount, number, or value of, to assess.[680]

Research is defined as a systematic investigation designed to develop or establish principles, facts or generalized knowledge, or any combination of them, and includes the development, testing and evaluation of research.[681]

3. Was the personal information provided explicitly or implicitly in confidence?

In confidence usually describes a situation of mutual trust in which private matters are relayed or reported. Information provided *in confidence* means that the supplier of the information has stipulated how the information can be disseminated.[682] In order for confidence to be found, there must be an implicit or explicit agreement or understanding of confidentiality on the part of both the local authority and the party providing the information.[683]

Implicitly means that the confidentiality is understood even though there is no actual statement of confidentiality, agreement, or other physical evidence of the understanding that the information will be kept confidential.[684]

---

[679] British Columbia Government Services, *FOIPPA Policy Definitions* at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions. Accessed April 23, 2020.
[680] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed.* at p. 493, (Oxford University Press).
[681] ON IPC Order PO-2693 at pp. 7 and 8. Definition originates from Ontario's *Personal Health Information Protection Act* (PHIPA) at section 2.
[682] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at p. 104, SK OIPC Review Reports F-2006-002 at [51], H-2008-002 at [73], ON IPC Order MO-1896 at p. 8.
[683] SK OIPC Review Reports F-2006-002 at [52], LA-2013-002 at [57]; ON IPC Order MO-1896 at p. 8.
[684] SK OIPC Review Reports F-2006-002 at [57], F-2009-001 at [62], F-2012-001/LA-2012-001 at [29], LA-2013-002 at [49], F-2014-002 at [47].

Explicitly means that the request for confidentiality has been clearly expressed, distinctly stated, or made definite. There may be documentary evidence that shows that the information was provided on the understanding that it would be kept confidential.[685]

Factors considered when determining whether a document was provided in confidence *implicitly* include (not exhaustive):

- What is the nature of the information? Would a reasonable person regard it as confidential? Would it ordinarily be kept confidential by the party providing it or by the local authority?[686]
- Was the information treated consistently in a manner that indicated a concern for its protection by the party providing it and the local authority from the point at which it was provided until the present time?[687]
- Is the information available from sources to which the public has access?[688]
- Does the local authority have any internal policies or procedures that speak to how records or information such as that in question are to be handled confidentially?
- Was there a mutual understanding that the information would be held in confidence? **Mutual understanding** means that the local authority and the party providing it both had the same understanding regarding the confidentiality of the information at the time it was provided. If one party intended the information to be kept confidential but the other did not, the information is not considered to have been provided in confidence. However, mutual understanding alone is not sufficient. Additional factors must exist in addition.[689]

The preceding factors are not a test but rather guidance on factors to consider. It is not an exhaustive list. Each case will require different supporting arguments. The bare assertion that the information was provided implicitly in confidence would not be sufficient.[690]

Factors to consider when determining if a document was provided in confidence *explicitly* include (not exhaustive):

---

[685] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 4 at pp. 104 and 105.
[686] BC IPC Orders 331-1999 at [8], F13-01 at [23]; NS IPC Review Reports 17-03 at [34], 16-09 at [44]; PEI IPC Order FI-16-006 at [19].
[687] ON IPC Orders PO-2273 at p. 8, PO-2283 at p. 10.
[688] ON IPC Orders PO-2273 at p. 8, PO-2283 at p. 10.
[689] *Jacques Whitford Environment Ltd. v. Canada (Minister of National Defence)*, 2001 FCT 556 at [40]; SK OIPC Review Reports F-2006-002 at [52], LA-2013-002 at [58] to [59]; ON IPC Order MO-1896 at p. 8; BC IPC Order F-11-08 at [32].
[690] SK OIPC Review Report LA-2013-002 at [60].

- the existence of an express condition of confidentiality between the local authority and the party providing it;[691]
- the fact that the local authority requested the information be provided in a sealed envelope and/or outlined its confidentiality intentions to the party prior to the information being provided.[692]

The preceding factors are not a test but rather guidance on factors to consider. It is not an exhaustive list. Each case will require different supporting arguments.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Section 31: Right of correction

Right of Correction

31(1) An individual who is given access to a record that contains personal information with respect to himself or herself is entitled:

(a) to request correction of the personal information contained in the record if the person believes that there is an error or omission in it;

(b) to require that a notation be made that a correction was requested but not made; or

(c) if the request has been disregarded, to be advised of the reason for which it has been disregarded.

(2) Within 30 days after a request pursuant to clause (1)(a) is received, the head shall advise the individual in writing that:

(a) the correction has been made;

(b) a notation pursuant to clause (1)(b) has been made; or

(c) the request has been disregarded, setting out the reason for which the request was disregarded pursuant to section 43.1.

[691] SK OIPC Review Reports F-2006-002 at [56], LA-2013-003 at [113], F-2014-002 at [47]; PEI IPC Order 03-006 at p. 5; AB IPC Orders 97-013 at [23] to [24], 2001-008 at [54].
[692] SK OIPC Review Reports F-2006-002 at [56], F-2012-001/LA-2012-001 at [29], LA-2013-002 at [49], LA-2013-003 at [113], F-2014-002 at [47]; PEI IPC Order 03-006 at p. 5; AB IPC Order 97-013 at [25].

(3) Section 12 applies, with any necessary modification, to the extension of the period set out in subsection (2).

Subsection 31(2) of LA FOIP provides local authorities with the options for responding to requests for correction. Within 30 days, the local authority must respond in writing giving its decision. See *Subsection 31(2)* of LA FOIP later in this Chapter for more guidance.

Subsection 31(3) of LA FOIP allows a local authority to extend the 30-day response period. See *Subsection 31(3)* of LA FOIP later in this Chapter for more guidance.

The right of correction was considered necessary because of the significance that personal information has for the ways in which local authorities deal with individuals in a wide variety of situations. Incorrect personal information in the hands of a local authority can have serious consequence for an individual in his or her dealings with the local authority, whether it be in relation to entitlement to benefits, suitability for employment or contracts or otherwise.[693]

The right provided to individuals by LA FOIP with regard to the correction of personal information about themselves is not an absolute right to require the correction of any such information that they consider to be incorrect. Such a right would leave local authority information subject to too great an extent, to the viewpoints of the individuals concerned. There will sometimes be uncertainty about whether particular information is correct or incorrect and independent verification may not be possible or feasible. The individual may take one view and the local authority another. In these circumstances, it would be inappropriate to require a local authority to "correct" its information to conform with the individual's view.[694]

What the right of correction does provide to individuals is a mechanism for requesting the correction of personal information about themselves when they believe that there is an error or omission in the information. The local authority in question is then free to make the correction desired or not, as it sees fit. If the correction is made, the individual concerned will have achieved his or her objective. If the local authority declines to make the requested

[693] Adapted from McNairn, C., Woodbury, C., 2009, *Government Information: Access and Privacy*, Carswell: Toronto, p. 8-28.
[694] McNairn, C., Woodbury, C., 2009, *Government Information: Access and Privacy*, Carswell: Toronto, p. 8-28.

correction, the local authority is required to make a notation in its records reflecting the correction that was requested but not made. In this way, it is intended that both the local authority's and the individual's versions will be on record and available to be taken into account whenever the information in question is used.[695]

Subsection 31(1)

Right of Correction

31(1) An individual who is given access to a record that contains personal information with respect to himself or herself is entitled:

(a) to request correction of the personal information contained in the record if the person believes that there is an error or omission in it;

(b) to require that a notation be made that a correction was requested but not made; or

(c) if the request has been disregarded, to be advised of the reason for which it has been disregarded.

Subsection 31(1) of LA FOIP provides individuals with three rights when it comes to correction of their personal information in the possession or control of a local authority:

1. The right to request personal information about them be corrected when there is an error or omission.

2. The right to request a notation be made on the record that a correction was requested but not made.

3. To be advised of the reasons when a request for correction has been disregarded under section 43.1 of LA FOIP

1. The right to request personal information about them be corrected when there is an error or omission.

[695] McNairn, C., Woodbury, C., 2009, *Government Information: Access and Privacy*, Carswell: Toronto, p. 8-28.

Subsection 31(1)(a) of LA FOIP provides that an individual is entitled to request correction of personal information where they believe there is an error or omission in it. The onus is on the individual to demonstrate to the local authority what the error or omission is.

A request for correction from an individual must, at a minimum:

- Identify the personal information the individual believes is in error. That personal information must be the personal information of the individual and not of a third party.
- The alleged error must be a factual error or omission.
- The request must include some evidence to support the allegation of error or omission. Mere assertions will not suffice.
- The proposed correction must be clearly stated and cannot be a substitution of opinion.[696]

The provision is not intended to function as an avenue of appeal, or redress, for an individual who is disappointed by a decision or disagrees with it.

2. The right to request a notation be made on the record that a correction was requested but not made.

Subsection 31(1)(b) of LA FOIP gives individual's the right to request a notation be made on the record indicating that a correction was requested but not made.

Notation is a note made on the individual's record by the personal information at issue or in an electronic record indicating that the individual has requested correction of the personal information. A notation should also include the date, who requested the correction, what the requested correction was and a signature or name of the decision-maker.[697]

3. To be advised of the reasons when a request for correction has been disregarded under section 43.1 of LA FOIP

Individuals have a right to make a request for correction of their personal information. However, there can be times when that right is abused.

---

[696] Office of the Nova Scotia Information and Privacy Commissioner (NS IPC) Review Report FI-09-79 at [13]. See also SK OIPC Review Report 147-2018, 197-2018, 008-2019, 073-2019/Investigation Report 192-2018, 221-2018, 058-2019 at [80].
[697] SK OIPC *Guide to HIPA* at p. 156. Available at IPC Guide to HIPA (oipc.sk.ca). Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 255.

Section 43.1 of LA FOIP provides for the ability to address those situations where the right to make a correction request is being abused.

To disregard a request for correction, a local authority must first make an application to the Commissioner requesting authorization to do so. The Commissioner will either grant or refuse the request.

If the request to disregard is granted by the Commissioner, the local authority can treat the correction request like it never happened. However, the individual still has a right to be notified that the correction request is being disregarded pursuant to subsection 31(1)(c) of LA FOIP.

Subsection 31(1)(c) is a relatively new provision that came into force January 1, 2018, following the amendments to LA FOIP. Section 43.1 of LA FOIP also came into force at the same time.

Subsection 31(2)

Right of Correction

31(2) Within 30 days after a request pursuant to clause (1)(a) is received, the head shall advise the individual in writing that:

(a) the correction has been made;

(b) a notation pursuant to clause (1)(b) has been made; or

(c) the request has been disregarded, setting out the reason for which the request was disregarded pursuant to section 43.1.

Subsection 31(2) of LA FOIP provides local authorities with the options for responding to a request for correction. Within 30 days, the local authority must respond in writing giving its decision.

The decision on how to proceed must be made and the individual advised in writing of the decision within 30 days of receiving the correction request. When determining the 30-day timeline for sending the response, *The Legislation Act* establishes general rules that govern the interpretation of all statutory instruments in the province of Saskatchewan. Section 2-28 of *The Legislation Act* provides the following for the computation of time:

2-28(1) A period expressed in days and described as beginning or ending on, at or with a specified day, or continuing to or until a specified day, includes the specified day.

(2) A period expressed in days and described as occurring before, after or from a specified day excludes the specified day.

(3) A period described by reference to a number of days between two events excludes the day on which the first event happens and includes the day on which the second event happens.

(4) In the calculation of time expressed as a number of clear days, weeks, months or years or as "at least" or "not less than" a number of days, weeks, months or years, the first and last days are excluded.

(5) A time limit for the doing of anything that falls or expires on a holiday is extended to include the next day that is not a holiday.

(6) A time limit for registering or filing documents or for doing anything else that falls or expires on a day on which the place for doing so is not open during its regular hours of business is extended to include the next day the place is open during its regular hours of business.[698]

Based on this, the following can be applied for calculating "*within 30 days after a request pursuant to clause (1)(a) is received*" under LA FOIP:

- The first day the request is received is excluded in the calculation of time [s. 2-28(2)].
- If the due date falls on a holiday, the time is extended to the next day that is not a holiday [s. 2-28(5)].
- If the due date falls on a weekend, the time is extended to the next day the office is open [s. 2-28(6)].
- As LA FOIP expresses the time in a number of days, this is interpreted as 30 calendar days, not business days.

[698] *The Legislation Act*, SS 2019, c L-10.2 at s. 2-28.

The Legislation Act does not allow for additional time for personal holidays, scheduled days off or if staff are away from the office due to illness.[699]

If the local authority does not respond to an individual within 30 days after receiving the request for correction, the individual has a right to request a review by the Commissioner pursuant to subsection 38(1)(c) of LA FOIP. For more on subsection 38(1)(c) of LA FOIP, see *Guide to LA FOIP*, Chapter 3: "Access to Records", *Section 38*.

Individual's may also request a review by the Commissioner if they disagree with the decision made by the local authority or if the local authority does not respond at all to the correction request.

In each case, the appropriate method for correcting personal information should be determined by taking into account the nature of the record, the method indicated by the applicant, if any, and the most practical and reasonable method in the circumstances.

There are three options for responding to a correction request:

1. Make the requested correction (s. 31(2)(a))

2. Make a notation on file (s. 31(2)(b))

3. Make an application to the Commissioner to authorize a disregard of the correction request pursuant to section 43.1 of LA FOIP

Subsection 31(2)(a)

Right of Correction
31(2) Within 30 days after a request pursuant to clause (1)(a) is received, the head shall advise the individual in writing that:

(a) the correction has been made;

When a local authority decides to correct an error, all records containing the personal information must be corrected. This includes records in all information systems - paper,

[699] SK OIPC Blog, *The Interpretation Act, 1995 – Things to Know*, June 7, 2017. *The Legislation Act* replaced *The Interpretation Act, 1995*. It came into force on May 15, 2019.

electronic and microform. Similarly, when the local authority decides to add omitted information, all systems must be updated. The record should be annotated with the date of the correction. A linking mechanism, as described below, may have to be employed when personal information is stored on a medium such as microform, which may be more difficult to update.[700]

For subsection 31(2)(a) of LA FOIP, the following criteria can be considered when deciding whether to make the correction requested:

1. Is the information at issue personal information?

2. Is there an error or omission?

3. Is the amendment a substitution of opinion?[701]

1. Is the information "personal information" as defined by LA FOIP?

For a correction to be made, the information at issue must qualify as "personal information" under LA FOIP.

Section 23 of LA FOIP defines "personal information".

For more on what qualifies as "personal information", see *Section 23*, earlier in this Chapter.

When considering requests for correction of personal information, it is important to distinguish between two types of personal information:

- *Factual information* about the individual, such as age, date of birth, income information or qualifications.
- *Opinions* about the individual, such as subjective assessments or evaluations of an individual's condition, abilities, or performance.[702]

2. Is there an error or omission?

---

[700] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 255.
[701] Original test appeared in SK OIPC Review Report F-2014-004 at [8] which originated from ON IPC Order MO-2766 at [89]. However, the second part of the test has been modified in this Guide to accurately reflect the language in LA FOIP.
[702] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 254.

An ***error*** is mistaken or wrong information or information that does not reflect the true state of affairs.[703]

An ***omission*** is information that is incomplete or missing or that has been overlooked.[704]

Factual information can be corrected. The individual must provide proof in support of the request for correction of factual information. Examples of documents that might be required to prove facts include a birth or baptismal certificate to prove age, or a notice of assessment from the Canada Revenue Agency to prove income.[705]

Factual information does not need to be corrected if the facts are in dispute and it is not possible to make a factual determination about the issue through the inquiry process.[706]

Opinions cannot be corrected. This includes professional and expert opinions.[707] See the third part of the test below.

Records of an investigatory nature cannot be said to be "incorrect", "in error", "incomplete", "inexact" or "ambiguous" if they simply reflect the views of the individuals whose impressions are being set out. In other words, it is not the truth of the recorded information that is determinative of whether a correction request should be granted, but rather whether what is recorded accurately reflected the author's observations, perception of events and impressions as they existed at the time the records were created.[708]

3. Is the amendment a substitution of opinion?

Opinions are not errors or omissions if they accurately reflected the views of the author at the time they were recorded, whether or not the opinion is supported by fact. The truth or falsity of the views or opinions is not the issue. A correction cannot be a substitution of opinion.[709]

---

[703] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 254. This definition was relied on in base case SK OIPC Review Report F-2014-004 at [20].
[704] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 254. This definition was relied on in base case SK OIPC Review Report F-2014-004 at [20].
[705] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 254.
[706] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 254.
[707] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 254.
[708] The base case for this provision was SK OIPC Review Report F-2014-004 at [23]. Originated from Ontario IPC Order MO-2766 at [91].
[709] AB IPC Order H2004-004 at [19].

Opinions are views or judgements not necessarily based on fact or knowledge.[710]

Professional opinions or observations are not normally subject to correction unless an error can be independently verified.[711]

> ***Professional*** means of or relating to or belonging to a profession.[712]
>
> ***Observation*** means a comment based on something one has seen, heard, or noticed, and the action or process of closely observing or monitoring.[713]

The significance of an opinion may be that it reflects another person's views at the time it was offered, and it may be important to have a record of that view at a later date. LA FOIP allows an individual to have his or her views about that opinion added to the record in the form of a notation instead of correction (see s. 31(b) below).

In each case, the appropriate method for correcting personal information should be determined by taking into account the nature of the record, the method indicated by the applicant, if any, and the most practical and reasonable method in the circumstances.

To **annotate** personal information means to add the requested corrections to the original record, close to the information under challenge by the applicant. An annotation should be signed and dated. When designing electronic forms and databases, provision should be made for allowing annotation.[714]

To **link** a record means to attach, join or connect the records to the requested correction. This may consist of a letter or statement from the applicant, or a copy of the request for correction.[715]

---

[710] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 999. See also SK OIPC Review Reports F-2006-004 at [43], LA-2013-003 at [26] and 139-2017 at [91].
[711] SK OIPC Review Report 125-2017 at [30].
[712] AB IPC Order H2004-004 at [19]. Originates from the Concise Oxford Dictionary, Tenth Edition.
[713] AB IPC Order H2004-004 at [19]. Originates from the Concise Oxford Dictionary, Tenth Edition.
[714] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 255.
[715] Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 255.

IPC Findings

In Review Report 011-2014, the Commissioner considered a request for correction made to the Village of Killaly (Village). The correction request was for a statement in a letter to the applicant from the acting clerk of the Village council. The Village did not make the correctio or make a notation that a correction had been correction. Upon review, the Commissioner found that the Village was not in compliance with subsection 32(2) of LA FOIP. The Commissioner recommended the Village make the correction requested by the applicant and advise the applicant of the correction pursuant to subsection 31(2)(a) of LA FOIP.

Subsection 31(2)(b)

Right of Correction
31(2) Within 30 days after a request pursuant to clause (1)(a) is received, the head shall advise the individual in writing that:

...

(b) a notation pursuant to clause (1)(b) has been made; or

Subsection 31(2)(b) of LA FOIP permits a local authority to make a notation on file where the decision was made not to correct the personal information.

Notation is a note made on the individual's record by the personal information at issue or in an electronic record indicating that the individual has requested correction of the personal information. A notation should also include the date, who requested the correction, what the requested correction was and a signature or name of the decision-maker.[716]

Notations should be:

- Permanent and obvious
- Should include:
    - The date
    - The name of the individual that requested the correction
    - What the requested correction was

[716] SK OIPC Guide to HIPA at p. 156. Available at IPC Guide to HIPA (oipc.sk.ca). Originated from Service Alberta, *FOIP Guidelines and Practices: 2009 Edition*, Chapter 7 at p. 255.

- A name or signature of the decision-maker
- The reason why the notation instead of the correction was made

IPC Findings

The Commissioner has not considered subsection 31(2)(b) of LA FOIP in a Report yet. However, the Commissioner has considered the equivalent provision in *The Freedom of Information and Protection of Privacy Act* (FOIP). Some examples are noted below:

In Review Report F-2014-004, the Commissioner considered a request for correction made to Saskatchewan Government Insurance (SGI). The correction request was for personal information to be changed or removed. SGI's decision was to not make the change but instead put a notation on the file pursuant to subsection 32(2)(b) of FOIP. The applicant did not agree with this decision and requested the Commissioner review it. This was the first time considering this provision in FOIP. The Commissioner determined that the information at issue was the personal information of the applicant. However, the Commissioner found that the information did not contain errors or omissions but was rather the views or impressions of the investigator as they existed at the time the record was created. Those views or impressions could not be said to be "inaccurate". Finally, the Commissioner determined that the applicant was requesting a removal or correction of the investigator's opinion. That being, the statement that the applicant was a "high moral risk" and he "flew under the radar for years". The Commissioner found that SGI's decision to place a notation on file and not correct the information was reasonable and that the information in question did not qualify for correction under subsection 32(1)(a) of FOIP.

In Review Report 069-2014, the Commissioner considered a request for correction made to the Public Service Commission (PSC). The correction request was for personal information (a date) in a Record of Employment to be changed. PSC's decision was to not make the change but instead put a notation on the file pursuant to subsection 32(2)(b) of FOIP. The applicant did not agree with this decision and requested the Commissioner review it. PSC asserted that the date was correct. The Commissioner found that the information was accurate, and that PSC responded appropriately to the applicant.

In Review Report 147-2018, 197-2018, 008-2019, 073-2019/Investigation Report 192-2018, 221-2018, 058-2019, the Commissioner considered a request for correction made to the Ministry of Justice (Justice). The correction request was personal information to be corrected on file. Specifically, that the applicant was associated with a Justice program. Justice denied the request and indicated there was no error or omission. Justice placed a notation on file instead pursuant to subsection 32(2)(b) of FOIP. The Commissioner found that the applicant

did not sufficiently identify the error or omission in the records nor provide supporting evidence to demonstrate there was indeed an error or omission. The Commissioner found that Justice appropriately responded to the correction request.

Subsection 31(2)(c)

Right of Correction
31(2) Within 30 days after a request pursuant to clause (1)(a) is received, the head shall advise the individual in writing that:

...
(c) the request has been disregarded, setting out the reason for which the request was disregarded pursuant to section 43.1.

Individuals have a right to make a request for correction of their personal information. However, there can be times when that right is abused.

Section 43.1 of LA FOIP provides for the ability to address those situations where the right to make a correction request is being abused.

To disregard a request for correction, a local authority must first make an application to the Commissioner requesting authorization to do so. The Commissioner will either grant or refuse the request. For guidance on how to make an application, see *Application to Disregard an Access to Information Request or Request for Correction*. See also *Guide to LA FOIP*, Chapter 3: "Access to Records", *Section 43.1*.

If the request to disregard is granted by the Commissioner, the local authority can treat the correction request like it never happened. However, the individual still has a right to be notified that the correction request is being disregarded pursuant to subsection 31(2)(c) of LA FOIP.

Subsection 31(2)(c) is a relatively new provision that came into force January 1, 2018, following the amendments to LA FOIP. Section 43.1 of LA FOIP also came into force at the same time.

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Subsection 31(3)

Right of Correction
31(3) Section 12 applies, with any necessary modification, to the extension of the period set out in subsection (2).

Subsection 31(3) of LA FOIP allows a local authority to extend the 30-day response period up to an additional 30 days where section 12 of LA FOIP authorizes the extension.

Section 12 of LA FOIP provides:

> **Extension of time**
> **12**(1) The head of a local authority may extend the period set out in section 7 or 11 for a reasonable period not exceeding 30 days:
>
> (a) where:
>
> (i) the application is for access to a large number of records or necessitates a search through a large number of records; or
>
> (ii) there is a large number of requests;
>
> and completing the work within the original period would unreasonably interfere with the operations of the local authority;
>
> (b) where consultations that are necessary to comply with the application cannot reasonably be completed within the original period; or
>
> (c) where a third party notice is required to be given pursuant to subsection 33(1).
>
> (2) A head who extends a period pursuant to subsection (1) shall give notice of the extension to the applicant within 30 days after the application is made.

(3) Within the period of extension, the head shall give written notice to the applicant in accordance with section 7.

For guidance on applying section 12, see *Guide to LA FOIP*, Chapter 3: "Access to Records", *Section 12*

IPC Findings

As of the issuing of this Chapter, the Commissioner has not considered this provision in a Report yet. This section will be updated accordingly when it is considered.

Section 38: Application for review

There are several provisions under section 38(1) of LA FOIP for which an applicant or individual may request a review or investigation by the Commissioner. As Chapter 6 focuses on privacy of personal information, only those provision relevant have been reproduced here. For more on section 38, see *Guide to LA FOIP*, Chapter 3: "Access to Records", *Section 38*.

Subsection 38(1)(a.4): Privacy complaints

Application for review

38(1) Where:

...

(a.4) an individual believes that his or her personal information has not been collected, used or disclosed in accordance with this Act or the regulations;

...

the applicant or individual may apply in the prescribed form and manner to the commissioner for a review of the matter.

Subsection 38(1)(a.4) of LA FOIP provides that an individual can request a review if the individual believes that his or her personal information has not been collected, used or disclosed in accordance with LA FOIP or *The Local Authority Freedom of Information and Protection of Privacy Regulations*.

The IPC refers to these reviews as "privacy breach investigations" and the individuals requesting them as "complainants".

Subsection 38(1)(a.4) of LA FOIP refers to a "prescribed form" that should be submitted to the Commissioner. Subsection 2(i) of LA FOIP provides:

> **2** In this Act:
>
> …
>
> (i) **"prescribed"** means prescribed in the regulations;

Individuals who wish to request an investigation by the Commissioner because they are not satisfied with how a local authority handled their privacy breach complaint, can do so using Form B found in the Appendix, Part II of *The Local Authority Freedom of Information and Protection of Privacy Regulations*. The form should be completed and provided to the IPC along with a copy of the local authority's response to the individual's privacy complaint. Any other relevant information, such as other communications with the local authority, can also be attached. The IPC will also accept requests that are not on Form B provided the request is in writing and contains the same elements of information as Form B.

Privacy in terms of 'information privacy' means the right of the individual to determine when, how and to what extent he or she will share information about him/herself with others. Privacy captures both security and confidentiality of personal information.[717]

A **privacy breach** happens when there is an unauthorized collection, use or disclosure of personal information, regardless of whether the personal information ends up in a third party's possession.[718]

An **unauthorized collection, use or disclosure** is one that does not comply with Part IV of LA FOIP. Part IV of LA FOIP contains the privacy provisions related to a local authority's handling of personal information of individuals.

The IPC is the office of last resort. For the Commissioner to consider a request for a privacy breach investigation, the complainant should take the following steps first:

---

[717] SK OIPC *2012-2013 Annual Report*, at Appendix 3.
[718] SK OIPC *2012-2013 Annual Report*, at Appendix 3.

1. The individual has made a written complaint to the local authority. Local authorities must have the opportunity to address an individual's privacy concerns first. It is only after this has occurred, and the individual is still not satisfied, that the IPC can investigate.

2. The local authority has responded (provide 30 days for a response). The IPC considers it reasonable to allow a local authority 30 days to respond to a privacy complaint. If an individual does not receive a response, it should follow up with the local authority.

3. Once a response is received from the local authority, if the individual is still not satisfied with how their concerns were handled, the individual can request the Commissioner investigate. The Commissioner cannot levy fines. The Commissioner's objective in an investigation is to assist local authorities with ensuring its policies and practices are compliant with LA FOIP. Outcomes of investigations where a privacy breach is found to have occurred generally, result in recommendations that policies and/or procedures be amended and/or individuals receive apologies for the breach.

To proceed, the Commissioner needs sufficient information and evidence that a breach of privacy may have occurred. When making the complaint, the following should be provided to the IPC:

1. A written complaint to the Commissioner:

    a. include details of the alleged breach; and
    b. attach any evidence that supports the complaint.

2. A copy of the response from the local authority.

For more on the role and authorities of the Commissioner see, *Guide to LA FOIP,* Chapter 2: "Administration of LA FOIP", *Information and Privacy Commissioner – Roles & Responsibilities.*

For more on the IPC process for an investigation, see *The Rules of Procedure*.

Subsection 38(1)(c): Correction reviews

Application for review

38(1) Where:

...

(c) an applicant requests a correction of personal information pursuant to clause 31(1)(a) and the correction is not made;

the applicant or individual may apply in the prescribed form and manner to the commissioner for a review of the matter.

Subsection 38(1)(c) of LA FOIP provides that an applicant can request a review where the applicant requested a local authority correct personal information and the local authority decided not to make the correction.

Applicants who wish to make a request for review because they are not satisfied with how a local authority handled their correction request, can do so using Form B found in the Appendix, Part II of *The Local Authority Freedom of Information and Protection of Privacy Regulations*. The form should be completed and provided to the IPC along with a copy of the local authority's response to the applicant's correction request. Any other relevant information, such as other communications with the local authority, can also be attached. The IPC will also accept requests for review that are not on Form B provided the request is in writing and contains the same elements of information as Form B.

For the Commissioner to conduct a review, the information must constitute the applicant's personal information. In addition, the applicant must be able to specify what information is incorrect and why.

For more on the right to request correction of personal information, see *Section 31* earlier in this Chapter.

Subsection 38(2): 1 Year Deadline

Application for review

38(2) An applicant or individual may make an application pursuant to subsection (1) within one year after being given written notice of the decision of the head or of the expiration of the time mentioned in clause (1)(b).

Subsection 38(2) of LA FOIP provides that applicants may make a request for review to the Commissioner within one year after being given written notice of the decision of the local authority.

Subsection 2-28(3) of *The Legislation Act*, provides that the first day is excluded in the calculation of time.[719] In addition, if the due date falls on a holiday, the due date falls on the next day that is not a holiday.[720]

If an applicant did not receive a response from the local authority, the applicant has one year from the 30th day under which the local authority was deemed to have responded pursuant to subsection 7(5) of LA FOIP.

Section 39: Review or refusal to review

There are several provisions under section 39(2) of LA FOIP for which the Commissioner can decide to refuse or discontinue a review or investigation. As Chapter 6 focuses on privacy of personal information, only the provision relevant has been reproduced here. For more on section 39, see *Guide to LA FOIP*, Chapter 3: "Access to Records", *Section 39*.

[719] Subsection 2-28(3) of *The Legislation Act*, SS 2019, c L-10.2 provides "A period described by reference to a number of days between two events excludes the day on which the first event happens and includes the day on which the second event happens".
[720] Subsection 2-28(5) of *The Legislation Act*, SS 2019, c L-10.2 provides "A time limit for the doing of anything that falls or expires on a holiday is extended to include the next day that is not a holiday".

Subsection 39(2)(a.6): Insufficient evidence

Review or refusal to review

39(2)(a.6) The commissioner may refuse to conduct a review or may discontinue a review if, in the opinion of the commissioner, the application for review:

…

(a.6) does not contain sufficient evidence;

Subsection 39(2)(a.6) of LA FOIP provides that the Commissioner can refuse or discontinue a review or investigation where the application does not contain sufficient evidence. This is a new provision that came into force on January 1, 2018.

Validity Test

There are times when a privacy complaint is received, and it needs to be tested for validity. To test for validity means to measure the degree of accuracy in the complaint to see if there is enough evidence to proceed with an investigation.

Validity means actually supporting the intended point or claim. To *validate* is to check or prove the validity of.[721]

To test validity, the following three questions can be considered:

1. What is alleged?

2. What argument and/or evidence was presented in support of the allegations?

3. Is there sufficient evidence to proceed with each part of the complaint?

When applying the validity test, consideration should be made of all facts and evidence provided.

When there is not enough evidence to proceed with a complaint, the complaint will be determined to be "not well founded".

---

[721] Pearsall, Judy, *Concise Oxford Dictionary*, *10th Ed*., (Oxford University Press) at p. 1583.

Privacy Impact Assessments (PIAs)

A Privacy Impact Assessment (PIA) is a diagnostic tool designed to help organizations assess their compliance with the privacy requirements in Saskatchewan legislation.[722]

One purpose of LA FOIP is to protect individuals against unauthorized collection, use and/or disclosure of their personal information in the possession or control of local authorities. An aspect of this duty to protect, is the duty to protect against any "reasonably anticipated" breaches of personal information (see *Section 23.1* earlier in this Chapter). A privacy impact assessment process is one tool that can help accomplish this.[723]

Privacy impact is where there are inadequate safeguards to protect personal information, or the legislation does not authorize collection, use, and/or disclosure of personal information.[724]

What is a Privacy Impact Assessment (PIA)?

A PIA is a process that assists organizations in assessing whether a project, program or process complies with the applicable access and privacy legislation. In Saskatchewan, local authorities are subject to LA FOIP. LA FOIP sets out rules as to how personal information is to be collected, used and/or disclosed. When a project, program or process is being designed, a PIA should be used to identify areas where there may be a privacy impact or risk.[725]

A PIA is <u>NOT</u>:

- A security assessment or a threat/risk assessment.
- A strategic planning exercise.
- An approval process.
- A privacy audit.

---

[722] SK OIPC Investigation Report F-2013-001 at [131].
[723] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-247. Available at Chapter (gov.mb.ca). Accessed December 17, 2022.
[724] SK OIPC resource *Privacy Impact Assessment: A Guidance Document* at p. 2. Available at Privacy Impact Assessment (oipc.sk.ca). Accessed December 17, 2022.
[725] SK OIPC resource *Privacy Impact Assessment: A Guidance Document* at p. 2. Available at Privacy Impact Assessment (oipc.sk.ca). Accessed December 17, 2022.

Why do a PIA?

- Risk mitigation
- Save time and money
- Confirms legal authority
- Marketing/communications
- Ethics
- There are risks associated with NOT doing one:
    - The risk to the privacy of individuals
    - Loss of public trust and confidence
    - Risk to services, programs, or activities – electronic systems in particular
    - Risk of the local authority and its employees being exposed to liability

When to complete a PIA:

Consider doing a PIA when you plan a:

- New system or administrative practice.
- Major change to an existing system or practice.
- Review of existing systems, services and practices to ensure that all privacy requirements continue to be met, identify new risks to privacy because of changing technology.

How to complete a PIA:[726]

A privacy assessment involves much more than completing a form or a checklist. It is an assessment, risk identification and risk mitigation process that requires a variety of skills.[727]

1. Gather the right team of experts, specialists, and advisors.

To carry it out properly, a variety of skill sets will be needed – such as program managers, technical specialists and privacy and legal advisors.

---

[726] The information that follows has been sourced and adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at pp. 6-251 to 253. Available at Chapter (gov.mb.ca). Accessed December 17, 2022.
[727] Adapted from Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-247. Available at Chapter (gov.mb.ca). Accessed December 17, 2022.

2. **At the outset, provide a detailed context.**

This should include:

- A detailed overview of the proposed initiative.
- A description of the underlying purposes and rationale for the initiative and of the need for personal information.
- A detailed description of the information to be collected, used and/or disclosed.
- A detailed description of the "information flow" – who will use it and for what purposes; to whom it will be disclosed and for what purposes; etc.
- An analysis of how the proposed collection and handling of personal information balances the benefits of the proposed initiative and the impact on individual privacy. Is the proposed initiative:

    - Necessary to achieve the intended purpose.
    - Effective in achieving the intended purpose.
    - Proportional that is, the loss of privacy is proportional to the benefit gained and there is no less privacy intrusive means of achieving the purpose.

      (See *Necessary, Effective & Proportional* earlier in this Chapter)

3. **Analyze, in detail, the "information flow" using privacy principles – and the questions that flow from these principles – as a framework.**

Each instance of collection, use, disclosure, retention, protection and disclosure of personal information must be 'tested' against the privacy principles that are reflected in LA FOIP. These principles are:

- Accountability
- Identifying purposes (and informing of purposes)
- Consent
- Limiting collection
- Limiting use, disclosure, and retention
- Accuracy
- Safeguarding
- Openness
- Individual access to and correcting one's own information

- Challenging compliance (monitoring for and challenging compliance).[728]

4. Use available tools as an aid, but don't be afraid to adjust them where necessary.

Adjustment to standard tools may be necessary if your local authority handles both personal information and personal health information, or if legislation other than LA FOIP applies to information maintained by your local authority.

The IPC has the following resources available to assist local authorities with completing a PIA:

Privacy Impact Assessment Guidance Document

PIA Step 1 – Preliminary Analysis

PIA Step 2 – Define the Project

PIA Step 3 – Privacy Analysis

PIA Step 4 - PIA Report

IPC Findings

In Investigation Report 034-2015, the Commissioner investigated an alleged breach of privacy involving the City of Saskatoon (City). The complaint alleged the City was recorded conversation of passengers on public City transit busses using audio surveillance. Upon investigation, the Commissioner found that the City had authority to collect the complainant's personal information. The Commissioner recommended the City undertake a privacy impact assessment exercise within three months of the issuance of the Report to ensure safety and security, and the PIA could inform policies and procedures that need to be created to ensure that the surveillance is being carried out in the most privacy protective manner.

[728] The principles are discussed earlier in this Chapter. See *10 Fair Information Principles*.

Records & Information Management (RIM)

Good records and information management (RIM) practices assist in the effective administration of LA FOIP.

Implementing strong RIM practices:

- Can prevent records from being lost or inappropriately deleted.
- Can ensure records remain legible and accessible.
- Can reduce search times and fees associated with finding mishandled information.
- Can reduce the risk of privacy breaches.

Poor RIM practices can impact your ability to:

- Respond to access to information or correction requests.
- Be transparent and accountable.
- Implement and maintain Open Data and Open Information programs.
- Ensure confidentiality and privacy of personal information.
- Meet any legislative requirements.

Basic RIM Concepts[729]

Understanding Records

Records can be emails, text messages, visual representations such as photographs, illustrations or maps, audio and video recordings, and data in any form. Consequently, RIM practices must address records in all their potential forms and media.

A challenge of introducing RIM practices is ensuring that staff understand the breadth of the term "record". Staff that deal solely with data, electronic files, or other formats of materials, must deal with their records in a similarly regimented way as staff dealing with traditional paper files.

[729] The remainder of this section originates from SK OIPC resource, *Improving Access and Privacy with Records and Information Management*. Available at improving-access-privacy-rim.pdf (oipc.sk.ca). Accessed December 17, 2022.

The Information Lifecycle

The "information lifecycle" refers to the various stages that records go through from their creation or acquisition to their final destruction or archiving. It is important to remember that access and privacy laws apply to records at any stage of their lifecycle. As a result, it is necessary to ensure that your RIM practices address each stage to protect and preserve valuable information.

Briefly, the information life cycle is:

1. **Creation and Collection:** This is the birth of a record. At this stage, a record is either created or collected. This can include several different types of records, such as drafts, research materials, and final versions of documents, data or analytics.

2. **Use and Maintenance:** Once a record has been created or collected, it enters this stage. Use and maintenance is typically focused on preserving records to ensure they remain accessible, legible and searchable. Their authenticity and integrity are preserved until they are approved for disposition.

3. **Disposition:** When a record is no longer useful, it will either be retained permanently (archived) or destroyed. The decision to archive or destroy the record will be based on historical assessment and evaluation of the record.

Records with a short-term value will generally be saved for a defined period before being destroyed, while records with a long-term value will be retained for a longer period and may be archived. Records that are deemed to be of no lasting value, such as transitory records, will be destroyed.

The method of destruction will vary depending on the sensitivity of the information contained within the record. For example, a publicly available newsletter may simply be recycled, whereas a document containing personal information or personal health information would require a secure destruction in accordance with records disposal policies.

RIM Best Practices[730]

The following RIM practices are commonly accepted best practices but are not exhaustive. The intention of this section is to provide local authorities with a high-level overview, rather than a detailed description of how to implement different RIM practices.

It must also be noted that no single approach will be appropriate for every local authority. Some of these practices will need to be modified to meet specific needs, and some may not be appropriate at all.

The IPC recommends that you work closely with your RIM staff in the development of practices that meet your organization's unique needs and situation. If your organization does not have dedicated RIM staff, consider designating a team or engaging with external consultants to investigate these options and develop an implementation plan.

1. Review and understand your organization's requirements

It is important to fully understand the recordkeeping rules that currently apply to your organization. Local authorities should ensure they consider any legislative requirements, policies or procedures related to records management or retention.

Implementing records retention schedules, policies and procedures are important to ensure the access to information and privacy rights of individuals are met. In consultation with your legal and RIM staff, review all existing requirements and how they have been implemented within your organization before considering new plans and RIM activities.

2. Develop safeguards

The information maintained within records will vary significantly, and as a result, not all records will require the same degree of protection. For example, personal information or personal health information must be protected from any unauthorized collection, use or disclosure. As a result of the requirements to protect personal information and personal health information, records that contain such information may require greater safeguards than others.

---

[730] The remainder of this section originates from SK OIPC resource, *Improving Access and Privacy with Records and Information Management*. Available at improving-access-privacy-rim.pdf (oipc.sk.ca). Accessed December 17, 2022.

Personal information, however, is only one form of information that may require special measures. The local authority may maintain records that are sensitive for other reasons. Consider, for example, law enforcement records that form part of an active investigation. The disclosure of this information may impede an investigation. Another example is location information for species at risk. The disclosure of this information could result in harm to an endangered species.

To effectively protect sensitive information, the local authority must know where that information is held, who may access it and under what circumstances. You can start by developing sensitivity classifications for your records and assign appropriate safeguards for each sensitivity level.

When implementing RIM practices and policies, it is essential to develop accompanying safeguard requirements. Records that contain personal information require several security controls. LA FOIP requires that local authorities have administrative, technical, and physical safeguards in place to protect personal information (see *Section 23.1*, earlier in this Chapter).

In addition to safeguards, consider data minimization and need-to-know at all stages of sensitive information handling (see *Need-to-Know Principle* and *Data Minimization Principle* earlier in this Chapter.

For more on this best practice see SK OIPC resource, *Improving Access and Privacy with Records and Information Management*.

3. Design with access and privacy in mind

When local authorities implement or plan to implement new information systems or technologies, it is essential that these tools be capable of functions that support access and privacy obligations under LA FOIP. When a system is not capable of simple extraction, the costs associated with an access or correction request may ultimately come at the expense of the local authority. Likewise, the lack of extraction capability could prevent the appropriate destruction or archiving of records, leading to potential privacy and access issues.

Consult with access and privacy staff, records management, legal and information technology staff before implementing a new system. The following may be taken into consideration when implementing a new system or technology:

- Conduct a privacy impact assessment to determine whether the risks outweigh the benefits and if all access and privacy legislation is being met. See *Privacy Impact Assessments (PIAs)* earlier in this Chapter.
- Determine if the system is compliant with your jurisdictional RIM requirements.
- Determine goals and objectives of the system or technology. Determine what needs to be collected to reach the desired outcome.
- Determine the structure and format of the data. For example, structured or unstructured fields.
- Determine if training will need to be done. Will the vendor demonstrate to the staff, or will simple on-site training be done.
- Following implementation, test the system. Are all access and privacy expectations being met.
- Determine when updates and maintenance should be completed.

For more on this best practice see SK OIPC resource, *Improving Access and Privacy with Records and Information Management*.

IPC Findings

In Review Report 035-2018, the Commissioner reviewed a denial of access by the Rural Municipality of Manitou Lake #442 (RM). An applicant requested access to all incoming and outgoing emails to the RM for the previous 18 months. The RM provided some emails to the applicant but also that some emails could not be located. The applicant requested a review by the Commissioner of the RM's search efforts. Upon review, the Commissioner determined that the RM's administrative assistant experienced resistance from a councillor when they were requested to provide copies of emails. As a result of the issues with the RM, the Commissioner recommended the RM create records management policies where councillors must promptly save emails that relate to RM business into a central records management system. Records, such as emails, related to RM business should be accessible to employees of the local authority to complete their duties under LA FOIP.

4. Designate staff as records management personnel

In large offices where many staff perform a variety of functions, it can be challenging to determine who is responsible for individual records. This challenge may grow over time, as staff change positions or leave the organization. This can become especially problematic

when access requests are received. If records have been abandoned, it can be extremely difficult for staff to identify the appropriate individuals and offices to conduct a search. Designating staff as records management personnel can help to address this issue.

Records management personnel are individuals or a group that is responsible for maintaining specific records or types of records. Depending on the nature of the records and the size of the organization, records management personnel may be an individual, a work unit or even a large branch. However, it is a best practice to identify a specific position or group that is most familiar with the records to be responsible for carrying out maintenance actions and responding to requests regarding the records.

When records management personnel for the organization have been identified, document the designation, and make the document accessible to others in the organization that may need-to-know. This can be done in several ways, depending on the types of records. For example, consider using metadata. Metadata is descriptive information about a data set or record which can easily include contact information for the responsible records management personnel. For some types of records, it may be appropriate to designate records management personnel in job descriptions, file plan documentation or simply as a note on a shared drive. It is important to remember to keep this information up to date, changing designations and contact information as necessary. The key point in designating records management personnel is to ensure that records are appropriately managed and maintained over time to prevent records from being mishandled, lost, or forgotten.

5. Develop and implement record schedules

Record schedules are tools that assist an organization in classifying, managing and disposing of their records. Schedules consist of a classification system to facilitate the systematic organization of records and a retention portion which establishes time periods for which records must be kept to meet all requirements. The retention portion also facilitates the disposition process.

These schedules are an essential component of any RIM strategy and must form part of the policies and procedures used to implement that strategy. LA FOIP does not specify retention and destruction periods. Therefore, local authorities that do not have a records retention schedule implemented or are unsure if they have any legislative requirements related to records retention, should consult with their RIM and/or legal staff.

6. Keep up with retention schedules

Establishing records retention schedules is an excellent first step in developing a RIM strategy, but to be fully effective, the schedules must be implemented and followed. As a starting point, train all staff on how to apply retention schedules to their records. This is particularly important for records management personnel who will be responsible for maintaining the records and ensuring that they are appropriately handled at the end of their lifecycle.

Once implemented, staff will need to periodically review holdings to find records that have exceeded their retention period and can be disposed of. Any records that are not accessed regularly can be moved to offsite storage where they are retained until they are eligible for disposal. Detailed inventories of records must be maintained. Records must be disposed of in accordance with the applicable records retention schedule following a well-established and well-documented disposal process.

The following tips can help your organization keep up with retention schedules and ensure that records are destroyed or archived properly.

1. Maintain detailed record inventories that include the dates the records are eligible for disposal and the appropriate schedule designations. This will allow records management personnel to quickly see which records have exceeded their retention period and what the next steps will be.
2. When large volumes of records are meeting their retention period at the same time, schedule reminders for staff.
3. Schedule regular record clean-up. This could be a large annual event or a smaller weekly task. Determine what kind of schedule works best and ensure that you keep up with the required schedule.
4. Identify transitory records and non-records and ensure they are destroyed in a consistent and regular manner.

Remember that records may be responsive to access requests if they are in the possession or control of the local authority. When staff are conducting reviews, it is important to remember that any records that are responsive to a request or subject to a litigation hold must not be destroyed. Ensure that staff consult with your local authority's RIM, legal and access to information departments before destroying records.

Office of the Saskatchewan Information and Privacy Commissioner. Guide to LA FOIP, Chapter 6, *Protection of Privacy*. Updated 27 February 2023.

7. Transitory records

Local authorities create and collect a large variety of records, but not all these records have ongoing value. Consider, for example, emails or posters about internal social events, or multiple copies of a report. While these records serve a short-term purpose, such as informing staff of a bake sale, or distributing copies of a report to many people, they do not serve any significant business purpose to the local authority or to the public. Records such as these are called **'transitory'** meaning that they are only useful for a short and temporary amount of time. These types of records may be used for simple tasks and have their own records retention schedule that allows them to be destroyed.

In developing and implementing RIM practices, it is vital that local authorities clearly define the difference between transitory records and non-transitory records and establish protocols for deleting transitory records. When an access request is received, staff may need to search through a multitude of record holdings. This task can be made significantly easier if transitory records are destroyed appropriately. The following considerations can help local authorities define transitory records:

- Was the record produced by your organization.
- Does the record document your organization's business. If the record contains information pertaining to your work, it is more likely to be a record that should be kept. If, however, the record pertains to internal social events, or external news clippings, it may not have a lasting value.
- Are there multiple copies of the same record. It is important to save the official copy of a record, but duplicates may not be needed.

Transitory records should be kept only for as long as they are needed. Destruction of transitory records that no longer have value reduces the amount of material being stored and the resources associated with storing and searching through unnecessary records. In addition, transitory records are subject to access to information requests and legal holds. For these reasons, local authorities should destroy transitory records on a regular basis. For more information on transitory records, check out the Provincial Archives of Saskatchewan's *Guidelines for the Management of Transitory Records*.

8. Email management

As described above, records can be in any format. Even though email is one of the main forms of business communication, many people see emails as inherently transitory. However,

business decisions, key communications and important information are regularly shared by email, and as a result, emails must be managed as any other record in accordance with the local authority's policies, legislative requirements, and records retention schedules.

Managing email records can be challenging, especially given the volume of emails received and sent. The following tips can help local authorities and their staff organize and manage their email records:

- Email messages that qualify as business records should be saved to shared repositories or other storage associated with the file in the institution's internal records keeping system. Determine what format will best suit your access and privacy needs and meets your RIM requirements and ensure that the format is stable and difficult to alter.
- When possible, avoid sending attachments. Rather, send hyperlinks to records in shared repositories to ensure that recipients have the most up to date version and to prevent potential inadvertent disclosure.
- Create folders within your email to organize emails into relevant subjects for your reference purposes. This can help keep inboxes manageable and may assist with workflow. Emails that are official records should be transferred and captured in your institution's internal records keeping system, ideally along with records they relate to, where they are retained in accordance with an approved records schedule.
- Keep subject lines short and clear, using consistent naming conventions when possible. This will help both you and the recipient find information and quickly identify relevant emails.

IPC Findings

In Review Report 301-2017, 302-2017, 303-2017, 304-2017, 003-2018, the Commissioner found that the Ministry of Central Services (Central Services) did not have an electronic filing system for the storage and organization of emails. The Commissioner recommended Central Services develop an email management policy or procedure to ensure emails are managed in the same manner as any other records.

In Review Report 035-2018, the Commissioner found the RM of Manitou Lake (the RM) had not made a reasonable effort to search for email records. The Commissioner made several recommendations regarding the management of email records including undertaking a records management project to ensure emails stored in council members' email accounts are

saved into the RM's central records management system and recommending the RM implement an email management policy.

9. Storage of electronic records

While records are in active use, they should be stored in a secure manner that allows for ease of access by authorized individuals. This is essential for responding to access requests as it can significantly reduce search time and resources. Shared drives, electronic records management systems or other shared organization storage resources are recommended, as they allow local authorities to set access controls and limit access to authorized individuals. When individuals save records on their assigned work computers or within their email or text messages, it is easy for those records to be lost should the computer break down, become lost or stolen or individuals leave the local authority.

Shared storage resources should have automatic back-up to prevent inadvertent loss of information. In addition, they should have security controls that allow only authorized individuals to access information. For example, access to a shared drive may be appropriate for members of a work unit or department but not for other members of the local authority. Alternatively, sensitive, or personal information or personal health information may require that only specific individuals or management have access.

10. File naming

File names are an important tool to help staff find information, especially in the context of an access request. However, when working on materials that are familiar to us, staff tend to use vague titles. While one staff member may easily recognize what "letter.doc" is, other staff will have to open the file to determine what the file actually is. In the context of an access request, this can result in significant search time and associated fees.

Implementing file naming conventions throughout a local authority can standardize the way that staff save file records and help ensure that materials can be easily searched for and accessed. File naming conventions do not need to be complicated to be effective. Rather, they should capture the minimum amount of information necessary for staff unfamiliar with the file to access it using a standard search.

Local authorities will need to consider the types of information that is necessary to easily identify records, but there are a few elements that are recommended:

- The date the record was prepared.
- A descriptive title. For example, rather than simply naming a document "New Practices," a more descriptive title could be "RIM Practice Guidelines."
- A version number as it can be easy to become confused when there are many versions of a record. Adding a version number can help ensure that staff are accessing the most current materials.
- Volume numbers if multiple files for a particular subject exist.

For more information concerning naming conventions, refer to the Provincial Archives of Saskatchewan resource *Naming Conventions*.

11. Entry and exit protocols

As staff move between positions and local authorities, it is easy for records to be lost, mishandled or destroyed inappropriately. Developing protocols for when staff start or leave positions can help prevent the loss of valuable information, as well as protect your organization from privacy breaches.

For staff entering a new position, ensure that they are made aware of the following:

- What records their position is responsible for maintaining.
- The RIM standards in place and how to apply them.
- Any mandatory or voluntary RIM training that is available.
- How to access and use shared organization storage resources.
- Who the contact is for questions about RIM.

For staff exiting a position, it is important to ensure that records created or maintained during the individual's tenure are appropriately saved, securely destroyed, or transferred to a replacement. Have the departing staff member or assigned staff member verify that the following is completed prior to their departure:

- Records have been stored, transferred to an archive, or destroyed based on their retention schedules following required disposal procedures.
- Personal non-work-related information that may have been stored on a computer or in paper files has been destroyed.
- Email records and text and picture messages have been appropriately saved in your organization's records keeping system or destroyed as per your organization's disposal requirements.

- A list of all records that the individual is responsible for maintaining has been prepared for transfer to the new records management personnel.
- Passwords for protected files or storage media have been reset and transferred to the new records management personnel.

Managers are responsible for ensuring that departing staff have completed all RIM requirements and should take steps to verify their completion.

12. Create a duty to document

As was seen above, records can be in any format. However, in some cases, important information is conveyed without the creation of a record. Business or policy decisions are sometimes made in meetings, over the telephone or in other settings that do not automatically create a lasting record (such as over instant messaging programs). When these decisions or actions are not recorded, local authority's may not be able to meet their access and privacy requirements. As such, local authorities should develop a policy requiring staff to document business or health service-related activities, including a duty to accurately document key decisions and actions.

In addition, it is important to ensure that staff use appropriate communication tools for business information. In IPC resource, *Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools*, the IPC also recommended that local authorities prohibit the use of non-local authority email accounts or instant messaging for conducting business or health services.

Implementing a requirement to document decisions and actions requires the development of policies and training for staff so that they will fully understand what information should be recorded and how to manage it.

Consider developing templates for use in specific situations, such as meeting notes or pre-developed nursing forms. Training on how and when to appropriately use these templates may help ease the transition for staff accustomed to making informal and undocumented decisions.

13. Ongoing training

Initial training on RIM practices is essential. It will provide your staff with a strong basis upon which to build additional knowledge and skills. However, for long-term practice changes to

take root, the lessons must be regularly refreshed and reinforced. Invest in a training program that allows staff to re-visit training materials and help them to understand RIM concepts and implement changes in their own work. Remember that the success of your RIM program is in the hands of your staff. Make sure that they have the resources and assistance that they need.

14. Review and audit

Implementing strong RIM practices should be a long-term goal. Do not expect quick and easy fixes. Staff are accustomed to their own filing and RIM practices, so changing habits can take a long time. As with any change, it will take time, patience and regular reinforcement.

To help keep staff accountable for maintaining RIM practices, it is highly recommended that local authorities include regular review and monitoring of RIM practices in their ongoing plans. In addition, including RIM actions and targets in annual performance plans will help keep staff engaged and accountable.

Conclusion[731]

By implementing RIM best practices, local authorities can vastly improve conditions for accessing information. Information that is appropriately created, managed and stored is eminently easier to find and use. In addition, following a well-documented disposal process regularly provides accountability for disposed information and reduces volume of information to search. Access requests can be processed with greater ease and efficiency. Staff time associated with record searches can be significantly reduced. Risks associated with failure to provide responsive records or with failing to meet the required response timelines can be avoided. Ultimately, a comprehensive RIM plan can help local authorities to be more agile, efficient, and accountable to the public.

Implementing RIM policies and practices can be challenging. Local authorities should establish effective procedures to manage their records over time, to engage staff and change ingrained habits. When preparing to develop and implement new or improved RIM practices, remember the following:

[731] The remainder of this section originates from SK OIPC resource, *Improving Access and Privacy with Records and Information Management*. Available at improving-access-privacy-rim.pdf (oipc.sk.ca). Accessed December 17, 2022.

1. **Compliance:** Make sure you follow RIM legislative requirements applicable to your local authority.

2. **Be engaged:** Senior management should understand the importance of RIM practices and actively support the efforts to introduce or update RIM practices.

3. **Communicate often:** It is essential to keep RIM practices top of mind to ensure that staff don't slip into old practices.

4. **Communicate clearly:** Communication and training on RIM should be clear and straightforward, using plenty of examples and real-world scenarios so that staff can fully understand their responsibilities and how to implement new practices.

5. **Commit to maintaining practices over time:** Implementing RIM practices is not a simple one-time event. It takes time and dedication to ensure that best practices become everyday practices.

IPC Findings

In Review Report 078-2016 to 091-2016, the Applicant received a fee estimate totaling $111,842.50 from the Global Transportation Hub Authority (GTH). The Commissioner found that the fee estimate was inappropriate as it was largely based on searching email archives, which would not have been an issue with effective records management policies and procedures in place. The Commissioner recommended GTH establish records management policies and procedures to ensure it is better equipped to handle access to information requests.

Record Retention

Local authorities collect personal information about citizens, employees, clients, and prospective clients. This information can be in physical or electronic form. Once this information has been collected, local authorities need to make informed choices about how long to keep it, and when and how to dispose of it.[732]

[732] Office of the Privacy Commissioner of Canada, *Personal Information Retention and Disposal: Principle and Best Practices*. June 2014. Available at Personal Information Retention and Disposal:

As local authorities get on the "Big Data" bandwagon, the push to amass enormous volumes of personal information for yet undetermined purposes has never been greater. The capacity and desirability to retain massive amounts of personal information indefinitely increases the risks and consequences of a potential data breach.[733] For more on "Big Data" see *Big Data* in the *Focus on Issues in Privacy* section later in this Chapter.

Control over the disposition of recorded information is an important aspect of records and information management that is critical to LA FOIP administration. Records retention and disposition schedules are a local authority's legal authorities on how long recorded information must be kept and how it is to be disposed of, e.g., by destruction or archival preservation.

Retention means to continue to have, hold, or keep personal information.[734]

Records schedule means a formal plan that identifies the public records that are subject to the plan, that establishes a classification system and retention periods for those public records and that provides for their disposition.[735]

LA FOIP does not specify how long a local authority should retain personal information. However, a specifically identified purpose is often a clear indicator of how long this information needs to be retained. There may be legislative requirements to keep information for a certain amount of time. In other instances, there may be no legislative requirement, and an organization needs to determine the appropriate retention period.

Check for a record retention and disposal schedule created by the Urban Municipal Administrators Association of Saskatchewan (UMAAS), the Rural Municipal Administrators' Association (RMAA), the Saskatchewan Urban Municipalities Association (SUMA) and the

---

Principles and Best Practices - Office of the Privacy Commissioner of Canada. Accessed December 19, 2022.

[733] Office of the Privacy Commissioner of Canada, *Personal Information Retention and Disposal: Principle and Best Practices.* June 2014. Available at Personal Information Retention and Disposal: Principles and Best Practices - Office of the Privacy Commissioner of Canada. Accessed December 19, 2022.

[734] Government of Manitoba, *FIPPA for Public Bodies – Resource Manual, Chapter 6, Protection of Privacy* at p. 6-106. Available at Chapter (gov.mb.ca). Accessed December 17, 2022.

[735] *The Archives and Public Records Management Act*, SS 2015, c A-26.11 at s. 2.

Saskatchewan Association of Rural Municipalities (SARM) with the assistance of the staff at the Provincial Archives.[736]

In assessing what is the appropriate retention period and whether it is time to dispose of personal information, an organization can consider the following points:

- Reviewing the purpose for having collected the personal information in the first place is generally helpful in assessing how long certain personal information should be retained.
- If personal information was used to make a decision about an individual, it should be retained for the legally required period of time thereafter – or other reasonable amount of time in the absence of legislative requirements – to allow the individual to access that information in order to understand, and possibly challenge, the basis for the decision.
- If retaining personal information any longer would result in a prejudice for the concerned individual or increase the risk and exposure of potential data breaches, the organization should consider safely disposing of it.[737]

Developing plain language internal policies and procedures that set out clear retention and disposal schedules – including minimum and maximum retention periods for the various types of personal information that are being held – is key. Internal policies should address the whole lifecycle of the personal information held by the organization.[738]

Contractors

Each local authority should have its own retention and disposition schedule that apply to records being maintained by a contractor on behalf of the local authority. Such retention and disposition schedules should be included as part of the contract. The contract should stipulate whether the records are to be transferred back to the local authority at the end of

---

[736] Provincial Archives of Saskatchewan, *Municipal Records*. Available at Municipal Records | Provincial Archives of Saskatchewan (saskarchives.com). Accessed February 17, 2023.
[737] Office of the Privacy Commissioner of Canada, *Personal Information Retention and Disposal: Principle and Best Practices*. June 2014. Available at Personal Information Retention and Disposal: Principles and Best Practices - Office of the Privacy Commissioner of Canada. Accessed December 19, 2022.
[738] Office of the Privacy Commissioner of Canada, *Personal Information Retention and Disposal: Principle and Best Practices*. June 2014. Available at Personal Information Retention and Disposal: Principles and Best Practices - Office of the Privacy Commissioner of Canada. Accessed December 19, 2022.

the retention period for destruction or the contractor is to destroy the records on behalf of the local authority. The contract should also state how the records are to be destroyed, including notification being provided to the local authority prior to destruction.[739]

Record Disposal

Destruction means to permanently destroy or erase in an irreversible manner to ensure that the record cannot be reconstructed in any way and does not include recycling or placing in the trash.[740]

Disposition includes the destruction of records, as well as appraisal and transfer to the Provincial Archives where needed. The disposal system is applicable to all formats, including digital.[741]

When responding to an LA FOIP request, it is necessary to know whether records have been destroyed and if so, whether this has been done in an authorized manner. It is equally important to dispose of personal information under conditions that protect the privacy rights of the individual.

Local authorities should include a provision in their record destruction polices that employees must obtain internal authorization prior to the destruction of personal information. The local authority could develop a process to authorize the destruction of batches of records on a single authorization. The authorization should include a signature field or sign-off and the level of authorization required.[742]

All too often, sensitive personal information intended for destruction is left in unsecured conditions and may be exposed to unauthorized access and, possibly, use. Examples include

---

[739] SK OIPC Investigation Report F-2013-001 at [68].
[740] ON IPC resource, *Get rid of it Securely to keep it Private: Best Practices for the Secure Destruction of Personal Health Information,* October 2009, at p. 3. Available at naid.pdf (ipc.on.ca). Accessed on December 17, 2022.
[741] Provincial Archives of Saskatchewan, Government of Saskatchewan Records Disposal System. Available at Government of Saskatchewan Records Disposal System | Provincial Archives of Saskatchewan (saskarchives.com). Accessed December 19, 2022.
[742] Adapted from SK OIPC Investigation Report H-2011-001 at [140]. Originated from ON IPC resource, *Get Rid of it Securely to Keep it Private – Best Practices for the Secure Destruction of Personal Health Information,* October 2009, at p. 9.

disposal of documents containing personal information in garbage bags that have been ripped open and disposal of personal information in a recycling container.[743]

Check for a record retention and disposal schedule created by the Urban Municipal Administrators Association of Saskatchewan (UMAAS), the Rural Municipal Administrators' Association (RMAA), the Saskatchewan Urban Municipalities Association (SUMA) and the Saskatchewan Association of Rural Municipalities (SARM) with the assistance of the staff at the Provincial Archives.[744]

Securely disposing of personal information

Authorized disposition of personal information can occur through:

- Transfer of records to the custody of the Provincial Archives of Saskatchewan or the archives of a local authority.
- Physical destruction of records containing personal information in such a way that it cannot be retrieved or reconstructed (e.g., cross-shredding).[745]

Securely disposing of electronic records

Used office and computer equipment poses a special risk. For example, filing cabinets moved to an auction centre with files containing personal information still inside or computer hard drives put up for auction with information still stored on them.

At a minimum, computer hard drives need to be professionally wiped clean of data before they are disposed of or sold.

Care should also be taken in the return or disposal of devices, such as facsimile machines, scanners, and photocopiers, that retain information in memory.[746]

---

[743] Service Alberta, *FOIP Guidelines and Practices, 2009 Edition*, Chapter 8 at p. 310.
[744] Provincial Archives of Saskatchewan, *Municipal Records*. Available at Municipal Records | Provincial Archives of Saskatchewan (saskarchives.com). Accessed February 17, 2023.
[745] Service Alberta, *FOIP Guidelines and Practices, 2009 Edition*, Chapter 8 at p. 310.
[746] Service Alberta, *FOIP Guidelines and Practices, 2009 Edition*, Chapter 8 at pp. 310 to 311.

Best Practices for the Secure Destruction of Personal Information[747]

A. Develop and Implement a Secure Destruction Policy

(i) Take a team approach

Organizations developing secure destruction policies should use a team approach by consulting internally with the organization's records management, risk management, information technology, security, privacy, facilities management and auditing departments. Secure destruction policies should be part of a complete Corporate Policy Manual that addresses all aspects of LA FOIP. Organizations may wish to also consult with legal counsel and potential service providers.

(ii) Determine in advance what records should be destroyed

An organization may choose to destroy records confirmed to have personal information only if the organization has very well-controlled and well-organized documentation regarding its information holdings. Alternatively, an organization may choose to securely destroy: 1) all records, 2) records where there is an absence of information about whether personal information is contained in the record(s) or 3) only those records where there is likelihood that personal information is contained, but it is impractical to confirm that fact (i.e., it would cost the same or more to confirm rather than securely destroy). These decisions should be made taking into consideration the types of records and the nature of the medium that may contain personal information.

(a) Types of records

The secure destruction policy should outline which types of records the policy applies to, such as stored records, duplicate records, incidental records and electronic media, as well as email and voice mail. Policies should refer to the organization's records retention and information classification policy in defining what information is to be considered confidential and should also require document labeling or access

[747] The following sections are adapted from ON IPC resource, *Get rid of it Securely to keep it Private: Best Practices for the Secure Destruction of Personal Health Information,* October 2009, at p. 3. Available at naid.pdf (ipc.on.ca). Accessed on December 17, 2022.

restrictions. Every organization has a 'daily waste stream' (or incidental records), usually paper, which is made of discarded records such as printing mistakes, notes and memos. This stream of records should be addressed in the secure destruction policy and should not be categorized as simple recycling if it may contain personal information.

(b) Types of media

Secure destruction policies must address all media that may be destroyed, including, but not limited to, paper, micro media (film media, such as microfilm and microfiche), magnetic tape media (reels, VCR, cassette), optical media (DVD, CD) and storage media (computers, hard drives, mobile phones, and portable memory devices). If office machines such as photocopiers, fax machines, scanners or printers contain storage devices, ensure that these devices are overwritten, erased, removed or destroyed when the machines are replaced. The policy should describe the specific methods for destroying each different type of media, the different internal authorizations for destruction, if any, and requirements for securing the media before destruction. If there are several accepted processes for destroying a type of media, the policy should identify the preferred process. For example, magnetic tape may be destroyed by degaussing, shredding or incineration, and the organization's policy should specify which method is to be used. See also 'Determine Best Methods of Destruction' section below.

(iii) Define roles and responsibilities

An organization's secure destruction policy should designate a policy compliance officer who will be the person ultimately responsible for organizational compliance, as well as compliance officers for each of the organization's physical locations. Ensuring compliance need not be a full-time job and can be simply part of an individual's job description to be responsible for the location complying with the organization's destruction policy. In addition to naming compliance officers, the policy should state that the employees' immediate supervisor is responsible for ensuring compliance with the policy daily. The policy should also name the individuals responsible for development of the policy, approval of the policy, employee orientation and training regarding the policy, contracting destruction services or equipment, performing internal audits, distributing updated policies and informing employees about updates. In addition, organizations should consider whether they wish to have someone witness the destruction. Note, some destruction companies offer the option for witnesses to view the destruction through a webcam over the Internet.

(iv) Consider the design of the secure destruction program

(a) In-house or outsourced

Deciding whether a secure destruction program should be conducted in-house, outsourced or partially outsourced is a key decision that each organization must determine and detail in their secure destruction policy. The policy should state that when contracting a service provider, the transfer of custody should be clearly documented, and the service provider must accept fiduciary responsibility for destroying the records. Organizations may wish to engage a secure destruction service provider that offers mobile or on-site destruction services. Whether destroyed internally or by a service provider, the individuals performing the destruction must be properly trained in the operation of the destruction equipment. Also, destruction must always be performed under secure and controlled conditions.

(b) Centralized or decentralized

Organizations performing an in-house destruction program should determine if the program will be centralized or decentralized. A centralized model of internal destruction involves employees collecting records to be destroyed in a container at their desk, where it is securely collected and transported by a designated employee to the location of the destruction equipment within the organization. In a centralized program, it may be a prudent policy to have some records isolated from the program and destroyed at the department level. A decentralized model of internal destruction involves employees destroying records themselves throughout the workday using equipment in the vicinity of their workstations. In this model, the organization may choose to have employees contact a specific person in the organization for large purges of paper. The decentralized model may be less suitable for very sensitive records as employees must be diligent in not leaving records or media unattended, as well as reporting any malfunctions in equipment to their supervisor. Regardless of which model is chosen for an organization's destruction program, this should be detailed in its secure destruction policy.

(v) Contingency planning

Policies should describe a contingency plan should a contracted secure destruction service provider suddenly not be available, or if destruction equipment such as a crosscut shredding machine ceases to operate. Some measures may increase the risk of theft, loss

and unauthorized use or disclosure, such as transferring records and media to another satellite location that has working equipment without a pre-established protocol to do so. Alternative measures may include keeping all materials to be shredded in a secure, clearly marked container until a new crosscut shredder is available. Or another secure destruction service provider may be contracted in accordance with an organization's criteria for choosing a service provider.

(vi) Application of the policy

A secure destruction policy should apply to all operating units of an organization, including remote operations, divisions or subsidiaries. The policy should document variations in the application of the policy, for example, if secure destruction is outsourced at a remote operating unit location but destroyed internally at a central location.

B. Segregate and Securely Store Personal Information

(i) Prior to destruction

Organizations must ensure that personal information in its custody or control is securely stored and protected against theft, loss and unauthorized use or disclosure. Also, that no unauthorized person will have access to the information between the time the records leave the organization until their actual destruction. As such, organizations should establish a procedure for segregating and securing personal information prior to destruction.

Once paper records have been segregated or stored prior to destruction, an organization may wish to isolate and label those records to lessen the possibility that there is unauthorized access or that they are disposed in an inappropriate manner (e.g., mistakenly placed in the recycling bin instead of destroying). Options for storing paper media include a secured workstation container or secured general office container kept in a separate location from all recycling bins.

Electronic media should also be segregated and secured. An organization may want to have satellite locations refrain from sending electronic media to another unit of the organization without detailed written permission from a designated individual within the organization. Organizations may wish to provide an easy point of contact for coordinating removal of electronic storage media from service such as hard drives.

(ii) After the destruction

Following degaussing or sanitization, access to electronic media must be restricted and further distribution delayed until an internal audit of a percentage random sampling of the media demonstrates that the degaussing or sanitization process was effective. Destroyed materials such as paper particles, after destruction, should be restricted from public access and eventually recycled to minimize heroic attempts at reconstruction.

C. Determine Best Methods of Destruction

The goal of record destruction is to have records containing any personal information permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. It is incumbent upon organizations to determine the destruction method that credibly implements their secure destruction policy requirements. Organizations must determine which destruction method is best suited to the classification of the record, taking into consideration cost and convenience as well as the sensitivity of the record. This determination will constitute the "approved methods of destruction" and should be detailed in the organization's secure destruction policy.

(i) Paper records

Methods of destroying paper include mechanical destruction (such as crosscut shredding, pulping, and pulverizing), and incineration. When mechanically destroying paper, material residue should be reduced to pieces millimeters in dimension. These pieces may be part of the organization's normal recycling program. When incinerated, material residue should be reduced to white ash and be contained so that partially burned pieces do not escape.

(ii) Electronic media

The method of destruction for electronic media includes mechanical destruction to render it unusable, degaussing and sanitization (including secure erase), and should involve removing all labels or markings that indicate previous use. Simply deleting computer files or reformatting a disk does not securely destroy the data because even deleted files may be subject to data recovery efforts.

For all personal hand-held computing or processing devices (such as PDAs and mobile phones) storing sensitive contact information, calendars, documents, email

correspondence and other information, methods of destruction may include mechanical destruction of the entire unit, or destruction of the replaceable memory circuits or card so that the device can be redeployed with a new memory component.

(iii) Employing more than one method

Organizations may wish to employ more than one method of destruction to ensure personal information cannot be reconstructed. For example, an organization may wish to go beyond shredding and ensure that pulverization or incineration of the records takes place in the case of paper records, or the physical destruction of degaussed or sanitized electronic media.

(iv) Organizational control

Organizations should take into consideration whether media will one day not be under their organization's control when determining which method of destruction should be chosen. For example, an organization wishing to return a hard drive for warranty purposes may wish to employ secure erase.

(v) Recycling does not equal secure disposal

When it comes to the disposal of personal information, recycling documents is not an acceptable option for secure destruction. In the recycling process, paper may be stored in warehouses for lengthy periods of time until enough has accumulated, and then may be sold while still intact. Remember, recycling does not equal secure destruction.

D. Document the Destruction Process

Documenting the destruction will assist in creating an audit trail for monitoring compliance with the organization's secure destruction policy.

(i) Authorization to destroy

Organizations should include in their secure destruction policies a provision that employees must obtain internal authorizations prior to the destruction of personal information. An organization may develop a process to authorize batches of records or media on a single authorization. The authorization should include a signature field for

sign off and the level of authorization required (e.g., specific department such as legal or audit). The authorization document may include the following information:

- Date of destruction
- Name, title, contact information and department of the person submitting the authorization
- Description of the information or media being destroyed
- Retention schedule reference number
- Any relevant serial numbers
- Quantity being destroyed
- Origination or acquisition year (can be a range)
- Retention expiration date
- Location of the records
- Reason for destruction
- Method of destruction
- Whether destruction is to be performed in-house
- Approved contractor and vendor number, if relevant
- Approved destruction method according to the organization's secure destruction policy

An organization may decide to exclude records not subject to the organization's retention schedule, such as incidental or duplicate records. However, organizations should note that without an internal authorization to destroy, further documentation should be substituted, for instance an internal log of the destruction or internally generated Certificate of Destruction issued on a routine basis (e.g., daily, weekly, etc.) to document the destruction of incidental or duplicate records. If outsourcing the destruction of incidental or duplicate records to a service provider, then the Certificate of Destruction or other transactional record, such as an invoice or service order, may act to provide documentation for audit trailing purposes.

(ii) Certificate of Destruction

Although it cannot serve as absolute proof that a destruction of records has taken place, a consistent and chronological series of Certificates of Destruction over an extended period may assist in establishing that the organization has adhered to its secure destruction policy. The policy should indicate the required fields in a Certificate of Destruction, whether produced by a secure destruction service provider or generated internally, and may include:

- Company name.
- A unique serialized transaction number.
- The transfer of custody.
- A reference to the terms and conditions.
- The acceptance of fiduciary responsibility.
- The date and time the information ceased to exist.
- The location of the destruction.
- The witness to the destruction.
- The method of destruction.
- A reference to compliance with the contract (if employing a secure destruction service provider).
- Signature.

Organizations creating internally generated Certificates of Destruction may also wish to include fields such as: who the destruction was conducted by (name, title, contact information, department, etc.); when collection of the information to be destroyed began (if using a centralized model of internal destruction); the type of media collected and from which specific containers; and the time at which the collection was completed. Regarding the destruction event itself, the internally generated Certificate of Destruction may detail the start time, location, equipment used, quantity destroyed and destruction completion time. An organization may develop a process to certify the destruction of batches of records or media.

(iii) Logs

In addition, creating a log for the destruction of records not subject to the organization's retention schedule, such as incidental and duplicate records, organizations may also include a provision in their secure destruction policy to create a record documenting the destination and disposal of the media particles following the destruction. In addition, the results of random sampling audits following the degaussing and sanitization process for electronic media should be logged.

E. Considerations Prior to Employing a Service Provider

(i) Criteria for choosing a service provider

Organizations should develop criteria for choosing a secure destruction service provider and include it in their secure destruction policy. For example, organizations may wish to

look for a provider accredited by an industrial trade association, such as the National Association for Information Destruction (NAID), or at least be willing to commit to upholding its principles. Criteria may also include finding a service provider that has written policies and procedures that must be approved by a specific person or committee within the organization. Additionally, criteria may also relate to whether the service provider creates a Certificate of Destruction for each destruction event, has a confidentiality agreement with each employee, and is willing to submit itself to independent audits.

(ii) Confirm method of destruction

Organizations outsourcing the secure destruction of paper and electronic media should include a requirement in their secure destruction policy to confirm which methods the potential service provider employs for the destruction of records.

(iii) Secure transportation

Organizations should confirm whether a potential service provider offers secure transportation of the materials to the destruction site, or whether the organization must obtain secure transportation services. Organizations should also develop procedures to ensure that the transfer of paper and electronic media for destruction is secure. When transferring to a secure destruction service provider, transfer procedures may include appropriately documenting transfer of custody and acceptance of fiduciary responsibility by the service provider or approved secure transportation carrier. Upon receipt of the media, the service provider should document and verify the reception of all media by checking serial numbers, etc.

An organization may wish to determine whether satellite locations will provide the paper records and electronic media to be destroyed directly to the approved service provider, or whether the satellite should ship the media to the central arm of the organization. If the satellite location deals directly with the service provider, the organization may choose to follow a procedure of having the authorization accompanying the records to the secure destruction facility, with a copy remaining at the satellite location.

(iv) Elements of a service provider contract

Organizations should sign a formal contract or agreement with all external service providers hired for the purpose of securely destroying records, or for transporting records

to be destroyed. This will ensure that all parties fully understand their respective roles and responsibilities.

An organization's secure destruction policy should specify the required elements of a service provider contract, and may include for example:

- The requirement that the service provider has written policies and procedures, which the organization should keep on file, and appended to the contract.
- That the service provider accepts fiduciary responsibility to protect and destroy the organization's materials in accordance with the service provider's written policies and procedures.
- That the service provider can demonstrate that it maintains indemnification coverage for any contractual liability it accepts.
- How the destruction will be accomplished, under what conditions and by whom.
- The time within which records collected from the organization will be destroyed and require secure storage pending such destruction.
- That a Certificate of Destruction be issued upon completion of the destruction.
- A provision that would allow the organization to witness the destruction, wherever it occurs, and to visit the service provider's facility.
- That there may be announced and unannounced audits of the service provider's processes to verify adherence to the service provider's written policies and procedures.
- That employees must be trained in and understand the importance of secure destruction of personal information.
- That the service provider must ensure the particles are disposed of in a secure manner and will not be placed at risk of unauthorized access.
- That the service provider must notify the organization ahead of time if any of the work is subcontracted to a third party, and that a written contractual agreement with the third party be consistent with the service provider's obligation to the organization.

F. Disposal of Securely Destroyed Materials

An organization's secure destruction policy should include a requirement to discard securely destroyed materials such as paper particles after destruction. Materials should be restricted from public access, and a record should be created documenting the destination and disposal of the media particles. Following degaussing or sanitization, access to the media must also be restricted and further distribution delayed until an internal audit of a percentage

random sampling of the media demonstrates that the degaussing and sanitization process was effective. It is up to the organization to determine the appropriate percentage for random sampling.

G. Auditing and Ensuring Compliance

Secure destruction policies and procedures must be applied consistently to be effective. Organizations should document violations of their secure destruction policy by employees and service providers, including a description of the violation, the nature of the media and any remedial action taken. The report of a violation can be given to the individual responsible for corporate security or human resources, or the supervisor responsible for the area where the violation occurred. Where the violation is a criminal act, a violation of contract or employment agreement, or involves the release of personal information, the organization should determine whether law enforcement, legal counsel or the Information and Privacy Commissioner of Saskatchewan should be contacted.

(i) Employee Compliance

Policies should detail how employee acceptance and championing of the secure destruction program will be obtained. Options for employee orientation and training may include a training class, completion of internet-based orientation training or self-study. Organizations should obtain from employees an acknowledgement to verify their understanding and agreement to comply with the secure destruction policy prior to handling any personal information. It should also be acknowledged by the employee that complying with the policy is a basis for continued employment, and that failure to adhere to the policy could result in disciplinary action or dismissal. The organization may wish to perform employee compliance audits where a designated individual, such as the employee's immediate supervisor, records findings such as whether collection containers are deployed and compliant, and whether unused electronic equipment is secured.

(ii) Service provider compliance

When developing a secure destruction policy, consideration should be given to how a contracted secure destruction service provider could be audited, including the frequency of audits. When performing an announced or unannounced audit of a service provider, the organization should check that criminal history screening or police background checks are performed, only authorized employees have access to records to be destroyed and the processing area, each employee signs a confidentiality agreement, and there are

written policies and procedures. To ensure compliance, an organization may choose to require the service provider file documents showing an update to policies and procedures, logs, employee screening and access control.

The service provider may offer verification of its current industry association certification status such as the National Association for Information Destruction (NAID) which may satisfy an organization's auditing requirement for secure destruction. NAID Certification is a voluntary program offered to its members. The program consists of an annual audit conducted by one of a network of independent security professionals who are accredited by ASIS International as Certified Protection Professionals. Professionals audit the applicant against the security standards of the NAID Certification Program. The program also includes unannounced, random audits of NAID Certified locations by the same security professionals.[748]

Preserving Records

The Provincial Archives collection includes municipal records from rural municipalities, towns, villages, and cities. The Archives collects municipal records through a records retention and disposal schedule which was created by the Urban Municipal Administrators Association of Saskatchewan (UMAAS), the Rural Municipal Administrators' Association (RMAA), the Saskatchewan Urban Municipalities Association (SUMA) and the Saskatchewan Association of Rural Municipalities (SARM) with the assistance of the staff at the Provincial Archives.[749]

Municipal records in the Provincial Archives' Collection document includes:

- the development, expansion, and growth of local communities.
- the relative prosperity of an area.
- local history over time (for example, community events and the history of community associations/organizations), including changes in the social and professional dynamics within the community.[750]

---

[748] The sections above were adapted from ON IPC resource, *Get rid of it Securely to keep it Private: Best Practices for the Secure Destruction of Personal Health Information,* October 2009. Available at naid.pdf (ipc.on.ca). Accessed on December 17, 2022.
[749] Provincial Archives of Saskatchewan, *Municipal Records*. Available at Municipal Records | Provincial Archives of Saskatchewan (saskarchives.com). Accessed February 17, 2023.
[750] Provincial Archives of Saskatchewan, *Municipal Records*. Available at Municipal Records | Provincial Archives of Saskatchewan (saskarchives.com). Accessed February 17, 2023.

Records from several municipalities have been preserved at the Archives in their original format or on microfilm. Although the collection contains records from all regions of the province, it is by no means comprehensive. For example, the cities of Saskatoon and Regina have each established their own archives program. Many types of records that the Provincial Archives would have collected in the past are now permanently retained by municipalities (for example, tax and assessment rolls), in accordance with legislation.[751]

Municipal records in the Archives' Collection include early assessment and tax rolls, municipal maps, as well as voters lists, budget information, improvement grants, feasibility studies, correspondence regarding ambulance and medical care, water quality/consumption reports, relief records, etc.[752]

For more on the preservation of records see the Provincial Archives of Saskatchewan.

Alberta IPC Investigation Report F2019-IR-02

In the Office of the Alberta Information and Privacy Commissioner (AB IPC) Investigation Report F2019-IR-02, the Commissioner determined that Alberta Justice and Solicitor General (JSG) did not preserve records responsive for two access to information requests. The Commissioner noted that when an applicant makes an access to information request, it triggers a duty on the government institution to preserve all potentially responsive records, including transitory records. The duty to preserve is fundamental to a government institution's duty to assist applicants. The Commissioner found that JSG failed to ensure that responsive records were preserved which compromised the integrity of the access to information process and did not comply with government's rules relating to the destruction of records.

[751] Provincial Archives of Saskatchewan, *Municipal Records*. Available at Municipal Records | Provincial Archives of Saskatchewan (saskarchives.com). Accessed February 17, 2023.
[752] Provincial Archives of Saskatchewan, *Municipal Records*. Available at Municipal Records | Provincial Archives of Saskatchewan (saskarchives.com). Accessed February 17, 2023.

Focus on Issues in Privacy

Big Data and Predictive Analytics

Big data refers to the sorting, matching, and analyzing of data sets to identify patterns, trends, and insights. Sometimes known as "data matching", the benefits of big data include policy development, system planning, resource allocation and performance monitoring.[753] It can also be used to analyze disease patterns and outbreaks as well as to detect fraud.

However, despite the benefits, big data impacts citizens' privacy by including the personal information and personal health information within the data sets used. Big data may enable governments to conduct surveillance on its citizens and how they live their lives.[754]

Predictive analytics is the identification of patterns and trends to predictive future behavior.[755] Predictive analytics can be used in areas such as law enforcement and policing but raises privacy concerns.[756]

Further, big data is critical for training and testing "artificial intelligence" systems. Professors David Poole, Alan Mackworth and Randy Goebel define **artificial intelligence (AI)** as "any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals".[757] AI raises fairness and privacy issues, especially when used by governments. AI systems have demonstrated bias and augments the ability to use personal information in ways that infringe privacy interests.[758]

---

[753] SK OIPC, *New Amendments (FOIP & LA FOIP)*, March 6, 2018. Available at PowerPoint Presentation (oipc.sk.ca) at p. 44. Accessed December 22, 2022.
[754] ON IPC resource, *Big Data and Your Privacy Rights,* available at fact-sheet-big-data-with-links.pdf (ipc.on.ca) at p. 2. Accessed December 22, 2022.
[755] BC IPC, *2015-2016 Annual Report*, available at 2173 (oipc.bc.ca) at p. 23. Accessed December 22, 2022.
[756] BC IPC, Leveraging the Transparency Effect in Police Governance, February 28, 2014. Available at 1624 (oipc.bc.ca) at p.3. Accessed December 22, 2022.
[757] BC IPC, *Getting Ahead of the Curve: Meeting the Challenges to Privacy and Fairness Arising from the Use of Artificial Intelligence in the Public Sector,* available at 3546 (oipc.bc.ca) at p. 5. Accessed December 22, 2022.
[758] BC IPC, *Getting Ahead of the Curve: Meeting the Challenges to Privacy and Fairness Arising from the Use of Artificial Intelligence in the Public Sector,* available at 3546 (oipc.bc.ca) at p. 1. Accessed December 22, 2022.

More recently, organizations have been considering the use of "synthetic data" to minimize the privacy impacts of big data but maximize the benefits. **Synthetic data** is a method of de-identifying data in a way that retains the same structure and level of granularity as the original data set.[759]

When embarking on big data initiatives, local authorities should make sure they are still meeting their privacy obligations under LA FOIP, including ensuring they have the authority to collect, use and/or disclose personal information under LA FOIP, as well as to ensure accuracy and completeness.

In the age of big data, it is increasingly important to understand the connection between the upstream collections, uses and disclosures of personal information and the downstream discriminatory impacts thereof. Data analytics – or any other type of profiling or categorization – that results in inferences being made about individuals or groups, with a view to profiling them in ways that could lead to discrimination based on prohibited grounds contrary to humans rights law, would not be considered appropriate.[760]

This is consistent with the spirit of the *International Resolution on Big Data* adopted by Data Protection and Privacy Commissioners around the world at their annual Conference in Mauritius in 2014. At this conference, Commissioners committed to calling on all parties to demonstrate that decisions around the use of Big Data were fair, transparent, and accountable. Also, that results from profiling be responsible, fair, and ethical. Finally, that injustice for individuals due to fully automated false positive or false negative results be avoided.[761]

For more information on this topic, see:

---

[759] Office of the Privacy Commissioner of Canada, *Privacy Tech-Know blog: When what is old is new again – The reality of synthetic data. Available* at Privacy Tech-Know blog: When what is old is new again – The reality of synthetic data - Office of the Privacy Commissioner of Canada. Accessed December 22, 2022.

[760] Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), 2. Profiling or categorization that leads to unfair, unethical, or discriminatory treatment contrary to human rights law.* Available at Guidance on inappropriate data practices: Interpretation and application of subsection 5(3) - Office of the Privacy Commissioner of Canada. Accessed December 22, 2022.

[761] Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), 2. Profiling or categorization that leads to unfair, unethical, or discriminatory treatment contrary to human rights law.* Available at Guidance on inappropriate data practices: Interpretation and application of subsection 5(3) - Office of the Privacy Commissioner of Canada. Accessed December 22, 2022.

Office of the Information and Privacy Commissioner of Saskatchewan

- *Data Matching* - data-matching.pdf (oipc.sk.ca)

Office of the Information and Privacy Commissioner of Ontario

- *Privacy Fact Sheet: Big Data and Your Privacy Rights*, January 2017: fact-sheet-big-data-with-links.pdf (ipc.on.ca)
- *Big Data Guidelines*, May 2017: bigdata-guidelines.pdf (ipc.on.ca)

Office of the Privacy Commissioner of Canada

- *Privacy Tech-Know blog: When what is old is new again – The reality of synthetic data*: Privacy Tech-Know blog: When what is old is new again – The reality of synthetic data - Office of the Privacy Commissioner of Canada
- *The Age of Big Data: A new, challenging frontier for privacy and our society:* Speech: The Age of Big Data A new, challenging frontier for privacy and our society - October 17, 2013 - Office of the Privacy Commissioner of Canada

Office of the Information and Privacy Commissioner of British Columbia

- *Annual Report 2015-2016*, Office of the Information and Privacy Commissioner for British Columbia: 2173 (oipc.bc.ca)
- *Leveraging the Transparency Effect in Police Governance*, Keynote Presentation to the BC Association of Police Boards, February 28, 2014: https://www.oipc.bc.ca/speeches/1624
- *Getting Ahead of the Curve: Meeting the challenges to privacy and fairness from the use of artificial intelligence in the public sector*: https://www.oipc.bc.ca/special-reports/3546.

Office of the Information and Privacy Commissioner of Nova Scotia

- *Big Data Guidelines for Nova Scotia:* Big Data Guidelines For Nova Scotia 2019 12 04.pdf

Surveillance Studies Centre, Queen's University

- *Big Data Surveillance* (2015 to 2020): Big Data Surveillance | The Surveillance Studies Centre (surveillance-studies.ca)

Biometrics and Facial Recognition

Biometrics refers to the technology of measuring, analyzing, and processing the digital representations of unique biological data and behavioral traits such as fingerprints, eye retinas, irises, voice and facial patterns, gaits, body odors and hand geometry.[762]

Facial recognition is the collection and processing of biometric facial data. It uses complex image processing techniques to detect and analyze the biometric features of an individual's face for the purposes of identification or verification of an individual's identity.[763]

A well-known case of the use of facial recognition that raised privacy concerns was the riots that occurred when the Vancouver Canucks lost in the Stanley Cup finals in June 2011. The Insurance Corporation of British Columbia (ICBC) offered the police the use of its facial recognition software to assist police in identifying individuals involved in the riots. The Office of the Information and Privacy Commissioner of British Columbia found that British Columbia's *Freedom of Information and Protection of Privacy Act* (BC FIPPA) did not authorize the change in use of ICBC's facial recognition database and ordered ICBC to immediately cease responding to requests from police to use its facial recognition database.[764]

Quebec is the only jurisdiction within Canada that has enacted legislation to govern the use of biometrics. Section 44 of Quebec's *Act to Establish a Legal Framework for Information Technology* limits the situations in which a person's identity may be verified or confirmed through biometric characteristic or measurements. Further, section 45 of the *Act to Establish a Legal Framework for Information Technology* requires organizations to inform Quebec's Commission d'accès à l'information (the Commission) of the creation of a database of biometric characteristics and measurements. It also allows the Commission to make orders regarding such databases. For more information, check out the Commission's website at: https://www.cai.gouv.qc.ca/biometrie/.

---

[762] BC IPC Investigation Report F12-01 at [35].
[763] Office of the Privacy Commissioner of Canada, Privacy guidance on facial recognition for police agencies, available at Privacy guidance on facial recognition for police agencies - Office of the Privacy Commissioner of Canada. Accessed December 22, 2022.
[764] BC IPC Investigation Report F12-01.

The Office of the Privacy Commissioner of Canada (OPC) describes the privacy principles of necessity and proportionality to ensure that privacy-invasive practices are carried out for a sufficiently important objective, and that they are narrowly tailored so as not to intrude on privacy rights more than is necessary. When determining necessity and proportionality of the use of facial recognition, local authorities should assess the following:

- Is facial recognition necessary to meet a specific need.
- Is facial recognition likely to be effective in meeting that need.
- Is the loss of privacy proportional to the benefit gained
- Is there a less privacy-intrusive way to achieving the same end.[765]

For more information on this topic, see:

Office of the Information and Privacy Commissioner of British Columbia

- *Investigation into the use of Facial Recognition Technology by the Insurance Corporation of British Columbia* (February 16, 2012): https://www.oipc.bc.ca/investigation-reports/1245

Office of the Privacy Commissioner of Canada

- *Privacy Guidance on Facial Recognition for Police Agencies* (May 2022): Privacy guidance on facial recognition for police agencies - Office of the Privacy Commissioner of Canada

Commission d'accès à l'information du Québec

- *Biométrie*: English | Commission d'accès à l'information du Québec (gouv.qc.ca)

Body Worn Cameras

Body worn cameras are recording devices designed to be worn on a law enforcement officer's uniform, which can include glasses or helmets. They provide an audio-visual record

[765] Office of the Privacy Commissioner of Canada, Privacy guidance on facial recognition for police agencies, available at Privacy guidance on facial recognition for police agencies - Office of the Privacy Commissioner of Canada. Accessed December 22, 2022.

of events from an officer's point of view as officers go about their daily duties. The high-resolution digital images allow for a clear view of individuals and are suited to running video analytics software, such as facial recognition. Microphones may be sensitive enough to capture not only the sounds associated with the situation being targeted but also ambient sound that could include the conversations of bystanders.[766]

Apart from requirements under personal information protection statutes, the use of body worn cameras can inform other obligations law enforcement agencies need to be aware. For example, body worn cameras can record video images, sound, and conversations with a high degree of clarity. Thus, there may be additional concerns raised under the *Canadian Charter of Rights and Freedoms*, the *Criminal Code* or provincial legislation, for example, whether the use of body worn cameras in any given context intrudes on the public's reasonable expectation of privacy or constitutes an interception of privacy communications, including in places accessible to members of the public. Law enforcement agencies also need to be mindful of additional legal implications whenever images and sound are recorded in private spaces, such as inside people's homes or vehicles.[767]

When considering whether to use body worn cameras, it is recommended that the necessity, effectiveness, and proportionality test be applied. See *Necessary, Effective & Proportional*, earlier in this Chapter.

For more information on this topic, see:

Office of the Information and Privacy Commissioner of Saskatchewan

- *Guidance for the Use of Body-Worn Cameras by Law Enforcement Authorities* (February 2015) - a document developed by the Office of the Privacy Commissioner of Canada in collaboration with the privacy oversight offices Alberta, New Brunswick, Quebec, British Columbia, Manitoba, Newfoundland and Labrador, Northwest Territories, Nova Scotia, Nunavut, Ontario, Prince Edward Island, Saskatchewan and Yukon: BWC guidance English latest version (oipc.sk.ca)
- *Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on police collecting personal information through bodycams,* June 21,

[766] SK OIPC, *Guidance for the Use of Body-Worn Cameras by Law Enforcement Authorities,* available at BWC guidance English latest version (oipc.sk.ca) at p. 1. Accessed December 22, 2022.
[767] SK OIPC, *Guidance for the Use of Body-Worn Cameras by Law Enforcement Authorities,* available at BWC guidance English latest version (oipc.sk.ca) at p. 1. Accessed December 22, 2022.

2020: Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on police collecting personal information through bodycams | IPC (oipc.sk.ca)

Office of the Information and Privacy Commissioner of Ontario

- *Model Governance Framework for Police Body-worn Camera Programs in Ontario*, June 2021: IPC Strategic Priorities 2021-2025

Data Brokers

Data brokers are companies whose primary business involves the trading and analysis of personal information. Specifically, data brokers are focused on the gathering and selling of consumer data for targeted marking purposes.[768]

Key actors include:

- Large online platforms such as Google and Facebook
- Marketers in the personal data and analytics industry
- Marketers in the risk analysis industry
- Other businesses spread throughout the economy, ranging from retailers to internet of things developers[769]

Sources of data for data brokers include:

- Newspapers
- Magazine publishers
- Books
- Music
- Movie clubs

---

[768] University of Ottawa, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), *On the Data Trail: How detailed information about you gets int o the hands of organizations with whom you have no relationship.* Available at Microsoft Word - Data Broker 06-07-06 _Color_.doc (cippic.ca) at p. 4. Accessed December 22, 2022.

[769] University of Ottawa, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), *Back On the Data Trail: The Evolution of Canada's Data Broker Industry.* Available at CIPPIC-Back_on_the_Data_Trail.pdf at p. 2. Accessed December 22, 2022.

- Mail order retailers
- Service providers
- Surveys
- Warranty cards
- Product registrations
- Contests
- Offers
- Loyalty cards
- Seminars
- Conferences
- Websites
- Non-profit and charitable organizations[770]

Opaque collection, accumulation and consolidation of consumer data has several privacy impacts. It is often unclear to what extent individuals are aware of, let alone consent to, the collection, use and disclosure of their personal information through these various channels.[771] Since 2006, technology has rapidly changed and advanced. New sources of consumer information now also include social media sites and search engines such as Google. There are significant challenges with protecting individuals' personal information from such data brokerage practices.

For more on this topic, see:

The Canadian Internet Policy and Public Interest Clinic (CIPPIC)

- *On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship*: Microsoft Word - Data Broker 06-07-06 _Color_.doc (cippic.ca)
- *Back on the Data Trail: The Evolution of Canada's Data Broker Industry:* CIPPIC-Back_on_the_Data_Trail.pdf

[770] University of Ottawa, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), *Back On the Data Trail: The Evolution of Canada's Data Broker Industry.* Available at CIPPIC-Back_on_the_Data_Trail.pdf at p. 2. Accessed December 22, 2022.
[771] University of Ottawa, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), *On the Data Trail: How detailed information about you gets int o the hands of organizations with whom you have no relationship.* Available at Microsoft Word - Data Broker 06-07-06 _Color_.doc (cippic.ca) at p. 47. Accessed December 22, 2022.

Personal Email Use for Business

Email is an easy and accessible form of communication and a tool that we all use in our professional and personal lives. However, for government-related activities, personal email accounts should not be used. There are both access and privacy issues that arise when government-related activities are conducted using personal email accounts.

LA FOIP provides individuals with the right to access records in the possession or under the control of a local authority, subject to limited and specific exemptions. Storing local authority records in personal email accounts, threatens the right of access to records that LA FOIP provides as searches for records responsive to an access to information request are not generally done of local authority officials' personal email accounts. There is also a risk that important records that reflect decision-making by local authorities are not preserved. Using personal email for government-related activities means the records reside elsewhere. A local authority should be taking steps to ensure that it is consistently preserving records in the name of good governance as well as for the responsible preservation of documents that could be subject to future access to information requests.[772]

Overall, such practices undermine the transparency and accountability of local authorities that is the foundation of access and privacy legislation. LA FOIP requires a local authority to respond to a written access to information request openly, accurately and completely (s. 5.1(1) of LA FOIP). The use of personal email accounts by public servants makes this duty difficult to comply with because local authorities may not be aware of the existence of records on personal email accounts that are responsive to an access to information request.

If an employee (councillor, mayor, etc.) uses a personal device and/or personal account (such as personal email account) to conduct government-related activities, the Commissioner has taken the position that such records are still subject to LA FOIP.[773]

The privacy implications when employees use personal email accounts to conduct local authority business must also be considered.

---

[772] SK OIPC Investigation Report 101-2017 at [34].
[773] SK OIPC resource, *Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools*, May 2018 at p. 4. Available at Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools (oipc.sk.ca). Accessed December 29, 2022.

Personal email accounts pose information security risks for local authority records. For example, records could end up stored on email servers that are outside of Canada. In instances where webmail services are used, such as "Gmail" or "Hotmail", email content is scanned and read to provide targeted advertising. Personal information in those records is not only stored outside Canada but it is also disclosed to the webmail provider. Local authorities are required under LA FOIP to take reasonable security measures to protect personal information from unauthorized access, collection, use or disclosure. When local authority records are stored in a personal email account with data servers located outside of Canada, the local authority no longer has control of how that information will be protected, disclosed, or accessed.[774]

The risks are not just with "Gmail" or "Hotmail" accounts. Email accounts with SaskTel ("sasktel.net") also have privacy considerations. SaskTel stores some data outside of Canada. It uses Google Apps for email and collaboration and stores some data in the Google Cloud. As some data is being stored outside of Canada, it may be subject to the laws of the countries where it resides.[775]

With the increased use of local authority assigned mobile devices and Bring Your Own Device (BYOD) programs, public servants are shifting from using the device for personal and local authority business increasing the risks of co-mingling information. Many public servants are unclear how to protect local authority records in such environments.

Email is not confidential by default, and personal information included in an email could be subject to a breach or unauthorized disclosure. It is important to note that in many instances, the technology used to send and receive email is not protected. Each delivery point between the recipient and the sender will store and forward the email and may do so in a plain, clear, and readable format. While it may only be technical people at each delivery point who would have the ability to read the email, there is a possibility that the delivery point could be breached, resulting in personal information being exposed.[776]

Personal email providers might not have adequate protections for personal information. If the information is sensitive, encryption can ensure the email is not readable along its journey.

---

[774] SK OIPC Investigation Report 101-2017 at [26].
[775] SK OIPC Investigation Report 101-2017 at [27].
[776] The Canadian Health Informatics Association (COACH) Guidelines, *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records – 2010 Guidelines for the Protection of Health Information Special Edition,* Canada's Health Informatics Association, 2020, p. 55. See also, SK OIPC Investigation Report 101-2017 at [29].

Digital signatures ensure accuracy by preventing the email contents from being tampered with or altered. The email system should be secure and meet current industry standards. The International Organization for Standardization (ISO) is the leading authority on international standards. ISO recommended the following with regards to electronic messaging:

> **13.2.3 Electronic messaging**
>
> Control
> Information involved in electronic messaging should be appropriately protected.
>
> Implementing guidance
> Information security considerations for electronic messaging should include the following:
>
> a) protecting messages from unauthorized access, modification, or denial of service commensurate with the classification scheme adopted by the organization.
>
> b) ensuring correct addressing and transportation of the message.
>
> c) reliability and availability of the service.
>
> d) legal considerations, for example requirements for electronic signatures.
>
> e) obtaining approval prior to using external public services such as instant messaging, social networking, or file sharing.
>
> f) stronger levels of authentication controlling access from publicly accessible network.[777]

When outside the local authority network, emails may be intercepted, may not be backed-up and may not have strong passwords.

Section 23.1 of LA FOIP explicitly requires local authorities to have adequate written policies and procedures in place that protect personal information against any reasonably anticipated threat or hazard to the security or integrity of the information. The policies and procedures

[777] International Organization for Standardization, *Information Technology*, ISO/IEC 27002, 2013. See also, SK OIPC Investigation Report 101-2017 at [30].

must address administrative, technical, and physical safeguards for personal information. See *Section 23.1* earlier in this Chapter for more on this requirement. Local authorities should have an email management policy.[778]

The Commissioner has addressed this issue with local authorities and government institutions in multiple reports which are summarized below:

> In Investigation Report 350-2017, the Commissioner investigated a complaint involving the Village of Hodgeville (Village). It was alleged that the Mayor of the Village forwarded a copy of the privacy complaint to personal email accounts including those of the councillors. This included "sasktel.net" and "hotmail.com" email addresses. The Commissioner recommended the Village set up email accounts for the councillors to use when conducting business for the village to ensure the security and retention of records.
>
> In Review Report 219-2018, the Commissioner discussed how a councillor was using a personal email account to conduct City of Moose Jaw business (City). To respond to an access to information request, the City requested the councillor to conduct a search of their personal email account using specific search terms and to provide the relevant emails. Even though the Commissioner was satisfied that the City verified with the councillor that the personal email account was searched for responsive records, the Commissioner recommended that the City set up email accounts for its councillors to use for conducting City business.
>
> In Review Report 361-2021, the Commissioner discussed how the text messages between the Administrator for the Village of Neudorf (Village) and two council members were responsive to an access to information request. The text messages were regarding Village business; however, the texts were sent from personal devices. The Commissioner found that the text messages would be subject to LA FOIP, and he recommended that the Village conduct a search for the responsive text messages on the personal devices. The Village had amended its practices by creating email accounts for its council members and discouraged the use of personal email accounts and personal cellular phones for Village business.
>
> In Review Report 184-2016, the Commissioner addressed the issue of Global Transportation Hub (GTH) board members using personal email addresses to conduct

[778] The Ministry of Central Services was in the process of developing a government wide email management policy in 2017. See SK OIPC Investigation Report 101-2017 at [37] to [38].

government-related activities. Board members received sensitive government documents at personal email addresses. The Commissioner recommended GTH board members use the Government of Saskatchewan email system for government-related activities.

In Review Report 051-2017, the Commissioner addressed the issue of the former Premier using a personal email account and a "saskparty.com" email account for government business. The Commissioner encouraged government leaders and public servants to use the Government of Saskatchewan email system to do government-related activities.

In Investigation Report 101-2017, the Commissioner investigated a complaint by an individual that alleged the Minister of the former Saskatchewan Transportation Company responded to the complainant using a personal/business email account. The Commissioner confirmed the alleged complaint and offered best practice advice with regards to the use of personal email for government-related activities.

In Review Report 216-2017, the Commissioner again raised concerns when it was learned that public servants with the Ministry of Economy (Economy) were using personal email accounts to conduct government-related activities. The Commissioner recommended that Economy prohibit its employees from using their personal email addresses for government-related activities and require them to use government-issued email accounts only.

In Investigation Report 262-2017, the Commissioner investigated a complaint involving the Ministry of Social Services (Social Services). CBC news articles reported concerns about the use of private email accounts for government business by Social Services. The Commissioner found that Social Services was using back-up tapes for the purposes of archiving official records which was not in compliance with *The Archives and Public Records Management Act* (APRMA). The Commissioner recommended that Social Services continue to work with Provincial Archives of Saskatchewan to develop an institution-wide records retention schedule to be compliant with APRMA and to ensure records are accessible for purposes of *The Freedom of Information and Protection of Privacy Act*.

For more information on this topic, see:

Office of the Information and Privacy Commissioner of Saskatchewan

- *Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and other Instant Messaging Tools: A Guide for Public Bodies*: Best Practices for

Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools (oipc.sk.ca)

- *Best Practices for the Management of Non-Work Related Personal Emails in Work-Issued Email Accounts:* Best Practices for the Management of Non-Work Related Personal Emails in Work-Issued Email Accounts (oipc.sk.ca)
- *Helpful Tips: Mobile Device Security:* Helpful Tips: Mobile Device Security (oipc.sk.ca)

Office of the Information and Privacy Commissioner of British Columbia

- *Use of Personal Email Accounts for Public Bodies:* 1515 (oipc.bc.ca)

Office of the Information and Privacy Commissioner for Nova Scotia

- *Instant Messaging and Personal Email Accounts,* September 2016: Instant Messaging Guide 2019 12 04.pdf (novascotia.ca)

Office of the Information and Privacy Commissioner of Ontario

- *Instant Messaging and Personal Email Accounts: Meeting Your Access and Privacy Obligations*, June 2016: Instant-Messaging.pdf (ipc.on.ca)

Snooping

Snooping, or the unauthorized access of personal information, occurs when employees access personal information or personal health information without a need-to-know. That is, they access personal information or personal health information for reasons beyond completing their job duties.

Snooping is a harmful and intrusive activity that undermines the trust citizens have in a local authority's ability to maintain the confidentiality of their information.

Many investigations undertaken into snooping cases by the Commissioner have resulted in recommendations that the government institution or local authority forward its file to the Public Prosecutions Division at the Ministry of Justice and Attorney General to determine if an

offence under *The Health Information Protection Act* (HIPA) has occurred and whether charges should be laid against the snooper.

In Investigation Report 228-2015, an employee had snooped on the personal information of 4,382 current and former SaskPower employees and copied files from that data. The Commissioner recommended that SaskPower forward its investigation file to the Public Prosecutions Division at the Ministry of Justice and Attorney General. Further, the Commissioner recommended that SaskPower report the matter to the employee's professional association.

The Commissioner has also investigated snooping cases where there have been unauthorized accesses into Saskatchewan Government Insurance's Auto Fund Database, including a matter where an employee of an issuer had been making unauthorized accesses since 1995. The Commissioner raised awareness around this issue in his blog, Insurance Brokers Snooping. In other jurisdictions, fines have been issued for snooping. For example, in Alberta:

- A pharmacist was fined $15,000 for inappropriately accessing information of individuals on Alberta's Netcare system.
- A former Alberta Health Services employee was fined $5,000 plus another $1,000 victim surcharge, for the inappropriate accessing of information of 189 individuals 985 times over a two-year period.
- A former Covenant Health employee was fined $3,000 for the inappropriate accessing of information on 16 individuals on 465 occasions.

In Ontario:

- A Masters of Social Work student was ordered to pay a $20,000 fine plus a $5,000 victim surcharge for snooping on the personal health information of five individuals.
- Two radiation therapists at University Health Network were ordered to pay $2,000 fines.
- A registration clerk at a regional hospital who snooped on 443 patients was ordered to pay a $10,000 fine.

Methods to deter snooping include local authorities establishing policies that set the expectation that employees are to only access personal information or personal health information that is necessary for their work. Local authorities should be delivering training on such policies and provide regular reminders of the expectation. Further, local authorities

should be conducting audits to ensure employees are accessing personal information appropriately.

For more information on this topic, see:

Office of the Information and Privacy Commissioner of Saskatchewan

- *Audit and Monitoring Guidelines for Trustees*, Office of the Information and Privacy Commissioner of Saskatchewan and eHealth Saskatchewan: https://oipc.sk.ca/assets/audit-and-monitoring-guidelines-for-trustees.pdf
- *Insurance Brokers Snooping*, Office of the Information and Privacy Commissioner of Saskatchewan (December 16, 2016): https://oipc.sk.ca/insurance-brokers-snooping/
- Investigation Report 228-2015 (SaskPower): https://oipc.sk.ca/assets/foip-investigation-228-2015.pdf – employee accessed the personal information of 4382 current and former SaskPower employees and copied two files from that data. Recommendation to forward file to Ministry of Justice, Public Prosecutions Division.

Office of the Information and Privacy Commissioner of Ontario

- *Snooping – Rights and Responsibilities*, (January 31, 2017): https://www.ipc.on.ca/wp-content/uploads/2017/02/2017-01-31-david-goodis-snooping.pdf
- *Protecting Personal Health Information*, (November 30, 2017): https://www.ipc.on.ca/wp-content/uploads/2017/11/2017-11-30-phipa-roto-windsor-web-2.pdf

Office of the Manitoba Ombudsman, Access and Privacy Division

- *Ten tips for Addressing Employee Snooping:* Ten Tips for Addressing Employee Snooping (ombudsman.mb.ca)

Surveillance

"If all that has to be done to win legal and social approval for surveillance is to point to a social problem and show that surveillance would help to cope with it, then there is no balancing at all, but only a qualifying procedure for a license to invade privacy."[779]

Surveillance is the close observation or listening of a person or place in the hope of gathering evidence.[780]

Video and audio surveillance systems are inherently privacy invasive, especially when used by local authorities. Surveillance systems enable governments to monitor and record individuals' actions and speech.

Many local authorities turn to video surveillance to help them fulfill their obligations to protect the safety of individuals and the security of their equipment and property. Video footage captured by cameras is regularly used to assist in the investigation of wrongdoing. However, the use of these surveillance technologies can put individuals' privacy at risk. Therefore, it is important to carefully consider both whether it is appropriate to install video surveillance and how it is used.[781]

Local authorities should ask if the surveillance system is necessary or if there is a less privacy-invasive option that achieves the same goal. Secondly, since surveillance systems collect personal information, local authorities should ensure it has the authority under LA FOIP to collect personal information or *The Health Information Protection Act* to collect personal health information. It should also consider if it has authority to use and/or disclose the personal information that is collected. Thirdly, local authorities must ensure it is meeting is obligations under LA FOIP. This includes notifying the public of the collection of personal information (subsection 25(2) of LA FOIP) the duty to protect (section 23.1 of LA FOIP) as well

---

[779] Alan Westin, Privacy and Freedom. Taken from ON IPC resource, *Guidelines for the Use of Video Surveillance*, October 2015 at p. 1. Available at 2015_Guidelines_Surveillance.pdf (ipc.on.ca). Accessed December 29, 2022.
[780] Garner, Bryan A., 2019. *Black's Law Dictionary, 11th Edition*. St. Paul, Minn.: West Group at p. 1746.
[781] ON IPC resource, *Guidelines for the Use of Video Surveillance*, October 2015 at main page introducing the resource. Available at Guidelines for the Use of Video Surveillance - IPC. Accessed December 29, 2022.

as having the ability to provide access to surveillance footage in response to access to information requests.[782]

Local authorities should ensure they are using surveillance systems in the most privacy protective manner as possible. This includes considering the location of surveillance systems. Areas where there are heightened expectations of privacy such as washrooms should not have surveillance systems.

Before implementing the use of video surveillance, some considerations are:

- Is the use of video surveillance lawful.
- Is the video surveillance necessary.
- Are there stakeholders to consult with.[783]

Once the decision is made to implement video surveillance, some considerations are:

- Is the duty to protect being met.
- What measures can be taken to minimize the impact to personal privacy.
- What safeguards should be put in place to properly protect the personal information.
- How will access to information requests for footage be handled.[784]

After the implementation, consideration should be made for the:

- Evaluation and audit of video surveillance programs.[785]

In Investigation Report 034-2015, the Commissioner investigated a complaint regarding the audio surveillance of passengers on the City of Saskatoon's (City) Access Transit busses. The Commissioner found that the City had authority to install audio surveillance on the busses for the purpose of reducing violence against transit operators, vandalism, and inappropriate customer behavior. The City had implemented practices to limit the privacy impacts on

---

[782] SK OIPC resource, *Video Surveillance Guidelines for Public Bodies*, January 2018. Available at Video Surveillance Guidelines for Public Bodies (oipc.sk.ca).
[783] For more see SK OIPC resource, *Video Surveillance Guidelines for Public Bodies*, January 2018. Available at Video Surveillance Guidelines for Public Bodies (oipc.sk.ca).
[784] For more see SK OIPC resource, *Video Surveillance Guidelines for Public Bodies*, January 2018. Available at Video Surveillance Guidelines for Public Bodies (oipc.sk.ca).
[785] For more see SK OIPC resource, *Video Surveillance Guidelines for Public Bodies*, January 2018. Available at Video Surveillance Guidelines for Public Bodies (oipc.sk.ca).

individuals including only retaining footage for a short period of time. Once the video digital recorder reached its capacity of 130 hours of footage, the system was looped and recorded over. Footage is only retrieved when there is an incident that is reported. Only the footage of the incident is retrieved and recorded to a disc or USB key. Otherwise, footage was not retrieved.

For more information on this topic, see:

Office of the Information and Privacy Commissioner of Saskatchewan

- *Video Surveillance Guidelines for Public Bodies* (January 2018): https://oipc.sk.ca/assets/video-surveillance-guidelines-for-public-bodies.pdf

Office of the Information and Privacy Commissioner of British Columbia

- *Public Sector Surveillance Guidelines*, (January 2014): https://www.oipc.bc.ca/guidance-documents/1601

Office of the Information and Privacy Commissioner of Ontario

- *Guidelines for the Use of Video Surveillance* (October 2015): 2015_Guidelines_Surveillance.pdf (ipc.on.ca)

Office of the Information and Privacy Commissioner of Nova Scotia

- *Video Surveillance Guidelines:* Video Surveillance Guidelines 2019 12 04.pdf (novascotia.ca)
- *Video Surveillance Policy Template:* Video Surveillance Policy Template 2019 12 04.pdf (novascotia.ca)

Office of the
Saskatchewan Information
And Privacy Commissioner

503 – 1801 Hamilton Street
Regina SK S4P 4B4
306-787-8350

www.oipc.sk.ca