PRIVACY BREACH GUIDELINES

for Government Institutions and Local Authorities

This document has two purposes. The first is to assist government institutions and local authorities (public bodies) to understand what a privacy breach is and how to deal with one. The second is to outline what to expect from a privacy breach investigation from the office of the Information and Privacy Commissioner (IPC). For more information, please see Part 4 and Part 6 of *The Rules of Procedure*.

Office of the
Saskatchewan Information
and Privacy Commissioner

May 2023

Contents

Privacy Breach Guidelines

There are two statutes that outline the privacy rules for government institutions and local authorities: *The Freedom of Information and Protection of Privacy Act* (FOIP) outlines rules for government institutions and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) outlines rules for local authorities. Trustees under *The Health Information Protection Act* (HIPA) should consult *Privacy Breach Guidelines for Trustees*.

What is a Privacy Breach?

What is Privacy?

"**Privacy**" can have many different meanings and has many dimensions. For more on privacy, see Chapter 6 of either the *Guide to FOIP* or *Guide to LA FOIP*. However, in the context of FOIP and LA FOIP, the focus is on data privacy, specifically, the protection of personal information. Personal information is defined in subsection 24(1) of FOIP and subsection 23(1) of LA FOIP.

When Does a Privacy Breach Occur?

A privacy breach is often thought of as inappropriate sharing of personal information, but generally, means a loss of or unauthorized collection, access to, use or disclosure of individually identifying personal information. A privacy breach can occur in a number of different ways.

Collection: A privacy breach could occur if a government institution or local authority collects personal information without authority under FOIP or LA FOIP. The rules for collection are found in sections 25 and 26 of FOIP and sections 24 and 25 of LA FOIP.

Use: A privacy breach could occur when personal information, already in the possession or control of the government institution or local authority, is used without authority under FOIP or LA FOIP. The rules for use are found in section 28 of FOIP and section 27 of LA FOIP.

Disclosure: A privacy breach occurs when an unauthorized disclosure of personal information transpires (e.g., when personal information is missing or when a government institution or local authority shares personal information with another organization without authority). Please note, if personal information in the possession or control of a government institution or 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, for instance, are found in sections 29 and 30 of FOIP and section 28 and 29 of LA FOIP and sections 16, 17 and 17.1 of *The Freedom of Information and Protection of Privacy Regulations* and sections 10 and 10.1 of *The Local Authority and Freedom of Information and Protection of Privacy Regulations*.

Accuracy: Government institutions and 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 27 of FOIP and section 26 of LA FOIP).

Other sub-issues: Other issues that might arise during a privacy breach investigation could include need-to-know, data minimization and consent. However, they would likely be tied to one of the other major issues.

Duty to Protect

FOIP and LA FOIP each include an explicit duty on government institutions and local authorities to protect personal information (see sections 24.1 of FOIP and 23.1 of LA FOIP) in their possession or control.

Sections 24.1 of FOIP and 23.1 of LA FOIP require that a government institution and local authority have administrative, technical and physical safeguards to protect personal information.

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 (IMSPs), auditing programs, records retention and destruction schedules, and access restrictions.

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

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.

Sections 24.1(a) of FOIP and 23.1(a) of LA FOIP indicate that a government institution and local authority must protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control.
Integrity refers to the condition of information being whole or complete, not modified, deleted or corrupted.

Confidentiality implies a trust relationship between the person supplying information and the individual or organization collecting or using it.

Subsections 24.1(b) of FOIP and 23.1(b) of LA FOIP indicate that government institutions and local authorities must protect against any reasonably anticipated:

- Threat or hazard to the security or integrity of the personal information in its possession or under its control.
- Loss of the personal information in its possession or under its control.
- Unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control.

Threat means a sign or cause of possible harm.

Hazard means a risk, peril or danger.

Security means a condition of safety or freedom from fear or danger.

A **need-to-know** is the principle that government institutions/local authorities and their staff should only collect, use or disclose the least amount of personal information needed for the purposes of the mandated service. 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.

Unauthorized access occurs when individuals have access to personal information that they do not need-to-know, either by accident or on purpose. This could also qualify as either an unauthorized use or unauthorized disclosure.

An **unauthorized collection** occurs when personal information is collected, acquired, received or obtained by any means for purposes that are not authorized under FOIP or LA FOIP.

Unauthorized use refers to the use of personal information for a purpose that is not

authorized by FOIP or LA FOIP.

Unauthorized disclosure refers to the act of revealing, showing, providing copies, selling, giving or relaying the content of personal information to third parties in ways that are not permitted by FOIP or LA FOIP.

Subsections 24.1(c) of FOIP and 23.1(c) of LA FOIP indicate that government institutions and local authorities should ensure its employees comply with the legislation. This means having education programs in place for their employees which cover the government institution's and local authority's duties under FOIP/LA FOIP including established safeguards, the need-to-know and data minimization principles and consequences for violating FOIP/LA FOIP. IPC has indicated that annual privacy and security training is a best practice.

There's Been a Privacy Breach: Now What?

If you have discovered or suspect a privacy breach, contact your organization's Privacy Officer immediately. Record all pertinent information related to the discovery of the breach.

If you have been tasked with dealing with the breach, consider the following steps.

Contain the Breach (as soon as possible)

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 Affected Individuals (as soon as possible)

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 the section on proactively reporting to the IPC later in this document)

- 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 both FOIP and LA FOIP require that, if there is an unauthorized use or disclosure of personal information, the government institution or local authority must notify the affected individual if the "incident creates a real risk of significant harm" to the affected individual (see sections 29.1 of FOIP or 28.1 of LA FOIP).

What is a **real risk of significant harm**? In terms of the advice from the Privacy Commissioner of Canada, the following is offered: "**significant harm"** includes 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.

The second consideration is whether there is a "real risk" that the significant harm will occur. Probability of harm and sensitivity of the personal information must be considered in making this determination. In terms of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the concept of sensitivity is discussed in Principle 4.3.4 as follows:

> Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a news magazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

For determining the probability that the personal information has been, is being, or will be, misused, further examination is required (see *What you need to know about mandatory reporting of breaches of security safeguards*). The Alberta IPC, in its *Personal Information Protection Act Mandatory Breach Reporting Tool*, offers the following factors to consider in analyzing the circumstances surrounding the breach when making this call:

- 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.

Does this mean that government institutions and local authorities only need to provide breach notification in the above cases? Not at all. A government institution or local authority needs to make that call in the course of investigating any privacy breach. And, in terms of whether to report to the IPC, this is always encouraged. Generally, if proactively reported, during its investigation, the IPC will consider how the government institution or local authority responded to the incident and if issues are sufficiently addressed, may resolve the matter informally without issuance of a formal public investigation report.

It is best practice to inform affected individuals and the IPC of breaches.

How to Notify Affected Individuals

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 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 them as a result 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.

Investigate the Breach

Once a breach has been contained the next step is to investigate the breach. 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.
- 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.

Take Steps to Prevent Future Breaches

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.

Privacy Breach Report

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.

The IPC will also request that government institutions and local authorities complete the IPC's *Privacy Breach Investigation Questionnaire* (*Questionnaire*), described later in this resource.

When Employee Snooping is Suspected

Sometimes the privacy breach involves an employee or contractor who purposely accessed personal information of individuals without a need to know. The following are steps or items to consider when investigating this type of breach:

- Record details of how the breach came to light.
- Suspend employee's access to the personal information.
- Retrieve log information if available.
- Interview the employee in question (establish if the employee may have shared their

user account and identification and routinely logged out of account).
- Identify and interview any witnesses.
- Review the privacy training the employee in question has received (have warnings of routine audits been given).
- Review any relevant contracts.
- Consider who needs to be notified (e.g., supervisor, union, police, etc.).
- Decide if the identity of the employee in question will be disclosed to the affected individual when providing notification.
- Proactively report to the IPC for further advice.

The IPC recommends that a government institution or local authority share any discipline measures taken against an employee who has snooped to the rest of the employees in the organization and the affected individuals. Please also include any details of employee discipline in your investigation report to the IPC.

What can I Expect if the IPC is Involved?

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 government institution's or local authority's actions or practices.
- A third party in possession of personal information could notify the IPC.
- Employees of a government institution or local authority inform the IPC of inappropriate practices within the organization.
- The IPC acts on media reports.
- The government institution or local authority proactively reports a breach to the IPC.

What Happens When a Government Institution or Local Authority Proactively Reports a Breach to the IPC?

Government institutions and local authorities should consider proactively reporting privacy breaches to the IPC. This means that when a government institution or local authority learns of a breach, it reports it to the IPC. While not mandatory, the IPC does encourage government institutions and local authorities to proactively report. To assist government institutions and 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*.

Advantages of Proactively Reporting

Some of the benefits 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 government institution/local authority on what to consider, what questions to ask and what parts of the legislation may be applicable.
- If the media asks, the government institution and local authority can assure the public that it is working with the IPC to address the matter.
- Should affected individuals contact the IPC, we can assure the individuals that we are working with your organization to address the breach which may prevent a formal complaint to the IPC.

What are the Possible Outcomes when I Proactively Report?

When a government institution or local authority proactively reports a privacy breach to the IPC, a file will be opened. The government institution or local authority will be asked to complete and provide the IPC's *Questionnaire* and other relevant material within 30 days.

The *Questionnaire* takes government institutions/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 our 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 government institution's/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, however, the breach is egregious, there is a systematic issue(s) involved, there is significant educational value or it involves a large number of affected individuals, the Commissioner may determine that a public report will be issued.
- Also, if an affected individual makes a formal complaint, the IPC will advise the public body and the Commissioner may determine that a public report will be issued.
- If the Commissioner is not satisfied with the government institution's or local authority's response, the IPC will issue a public report.

Once the IPC has made a decision, the government institution or local authority will be advised if a report will be issued or not.

Summary of Investigation Process

1. A privacy complaint is received by the IPC or a government institution or local authority proactively reports a breach to the IPC. It will be assigned to an Intake Officer.
2. The Intake Officer will ensure all necessary information has been received from the complainant, government institution/local authority, or other parties. When there is a complainant, the Intake Officer will attempt early resolution between the parties.
3. If early resolution is not possible, the Intake Officer will send out notice of the investigation via email or letter to all parties involved. It will request that the government institution/local authority complete the *Questionnaire* and provide any relevant materials in 30 calendar days. Relevant materials can include copies of relevant policies and/or procedures and/or agreements (or plans to develop relevant polices and/or procedures and/or agreements) or any other relevant documentation.
4. The file will be transferred to an Analyst. The Analyst will ensure materials arrive in 30 calendar days. If materials are not received in 30 calendar days, or an agreed upon deadline, the escalation guidelines are as follows:
    - The Analyst will follow up and attempt to receive materials.
    - The Analyst will escalate to the Director of Compliance (DoC) or the Executive Director of Research, Policy and Compliance (EDRPC).
    - If necessary, the DoC/EDRPC will escalate to the Deputy Commissioner or the Commissioner, who may contact the 'head'.
5. The Analyst will review materials received and do some initial analysis to determine the direction of the investigation.
6. The Analyst will meet with the DoC or EDRPC to whom they report, the Deputy Commissioner, and/or with the Commissioner to discuss the proposed direction. Informal resolution may be attempted. If successful, the file will be closed informally, without a report. Otherwise, the Analyst will start working on the report.

    If it is a proactively reported breach, the Analyst will review materials received and after consulting with the DoC/EDRPC, present findings and recommendations to the Deputy Commissioner and Commissioner. The possible outcomes are as follows:

    - If the Commissioner is satisfied with the government institution's or local authority's overall response to the breach, the file will be closed informally and

without a public report. This process may include some informal recommendations from the IPC.

- If, however, the Commissioner is satisfied with the government institution's or local authority's overall response to the breach, but the breach is egregious, there is a systematic issue involved, there is significant educational value or it involves a large number of affected individuals, the IPC may determine that a report will be issued.
- If the Commissioner is satisfied with the government institution's or local authority's overall response to the breach, but an affected individual makes a formal complaint, the IPC may determine that a report will be issued.

If the IPC decides to close the file informally, the Analyst will notify the parties. Otherwise, the Analyst will notify the government institution or local authority if the IPC has decided to issue a report.

7. The Analyst will draft a report and send it to the Deputy Commissioner and the Commissioner for final approval.
8. The Analyst will email the final report to any complainant(s) and government institution or local authority.
    - One copy of the final report will go to the complainant(s).
    - Another copy of the final report will be emailed to the government institution or local authority:
        - The email will be sent to the Head.
        - The email will be copied to the Privacy Officer.
        - Additionally, copies of the final report will be sent to the Deputy Minister of Justice, other relevant Deputy Ministers and any others as directed by the Commissioner.

    The Report is now issued.
9. As of September 1, 2022, all reports will be posted to the website on or after seven days of issuance, unless the Commissioner directs otherwise.
10. Sections 49 and 55 of FOIP (sections 38 or 44 of LA FOIP) require a government institution or local authority to respond to the Commissioner's final report within 30 days. It must also provide a copy of its response to any complainant(s). Pursuant to section 56 of FOIP (section 45 of LA FOIP), the response must be sent within 30 days of the issuance of the report. Government institution and local authority responses are tracked by the IPC.
11. Government institutions and local authorities should also be aware that, because of the amendments described above, a complainant can appeal the government

institution or local authority's decision to the Court of King's Bench (see section 57 of FOIP and section 46 of LA FOIP).

Early Resolution

Where possible, the IPC will aim to achieve early resolution for investigation files. Early resolution is beneficial to all parties involved as it can expedite resolution for the complainant and reduce the amount of work for both the government institution/local authority and the IPC.

When the IPC first receives a privacy complaint, it will receive a file number and be assigned to an Intake Officer. The Intake Officer will first verify that the IPC has received all the necessary information and documents from the complainant. The Intake Officer will then contact both the complainant and the government institution/local authority to facilitate a possible early resolution.

Some of the ways an Intake Officer might facilitate an early resolution are as follows:

- Dispel any misunderstandings.
- Clarify the complainant's objectives with the government institution/local authority.
- Clarify the role of the IPC.
- Identify possible outcomes of an investigation.

If an Intake Officer is not able to reach early resolution, notification letters/emails will be sent, and the file will be assigned to an Analyst. However, the IPC will be open to reaching informal resolution at any stage of the investigation process.

If the IPC is satisfied with a government institution's or local authority's internal investigation report, we may close the file rather than conduct a formal investigation.

When early resolution is achieved, the Commissioner will not issue an investigation report.

What will be the IPC's Focus?

The IPC will look at all the elements of the breach. However, focus will be on the following areas:

- The duty to protect (did the government institution/local authority meet the duty to protect)
- Compliance with the applicable legislation
- Safeguards, policies and procedures in place at the time of the breach (were they followed and were they effective)

- Training of the employees involved
- Potential employee snooping (if applicable)

The key questions for a privacy breach investigation can be found in the *Questionnaire*. It captures most issues the IPC routinely considers during our investigation. However, every investigation is unique. It is not unusual for an Analyst to ask further questions of a government institution or local authority during the process.

It is important to also provide the IPC with relevant documentation such as policies and procedures, training materials, copies of the personal information in question, etc.

Commissioner's Report

The Commissioner will issue a report for every investigation file that is not resolved informally. A copy of the investigation report may also be sent to the Ministry of Justice and any other relevant ministries or associations such as the Saskatchewan School Boards Association, Saskatchewan Association of Rural Municipalities or Saskatchewan Municipalities Association. See Part 6-10(1) of *The Rules of Procedure* for organizations that may receive a copy of the report.

As indicated earlier, all Reports will be posted on the IPC website within seven days from issuance.

FOIP and LA FOIP require that the government institution/local authority provide a response to the report and recommendations within 30 days to the relevant parties.

Contact Information

If you have any questions or concerns, please contact our office at:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC