PRIVACY BREACH GUIDELINES

for Government Institutions and Local Authorities

This document has two purposes. The first is to assist government institutions and local authorities 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).

May 2018

Office of the
Saskatchewan Information
and Privacy Commissioner

Privacy Breach Guidelines

There are two statutes that outline the privacy rules for public bodies. *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*.

Contents

WHAT IS A PRIVACY BREACH?

What is Privacy?

"Privacy" can have many different meanings. However, in the context of FOIP and LA FOIP, the focus is on information privacy; the right of an individual to determine for him/herself when, how and to what extent his/her personal information or personal health information will be shared.

Personal information is defined in section 24 of FOIP and section 23 of LA FOIP. Personal health information is different from personal information. Personal health information is defined in subsection 2(m) of HIPA.

When does a Privacy Breach Occur?

A privacy breach is often thought of as inappropriate sharing of personal information. However, a privacy breach can occur in a number of different ways:

Collection: A privacy breach could occur if a public body asks for or collects more personal information needed for the purpose for which it is being collected (e.g. a health services number is required for a non-health related service, social insurance number is required to make a job application, personal information is not collected directly from the individual, etc.). 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 public body is used for reasons that are not consistent with the purpose for which they were collected (e.g. personal information is collected to provide one service and then used to promote a different service). The rules for use are found in sections 28 of FOIP and 27 of LA FOIP.

Disclosure: A privacy breach could occur when an unauthorized disclosure of personal information transpires (e.g. when personal information is missing, when an employee accesses personal information without a need-to-know, when a public body shares personal information with another organization, etc.). Note: if personal information in the possession or control of a public body 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 29 of FOIP and 28 of LA FOIP.

Accuracy: Public bodies 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 sections 27 of FOIP and 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, LA FOIP and their Regulations provide reasons a public body should collect, use and disclose personal information. Any collections, uses or disclosures unauthorized by FOIP or LA FOIP would be a privacy breach. Additionally, effective January 1, 2018, an amendment to FOIP and LA FOIP added an explicit duty on public bodies to protect personal information (see section 24.1 of FOIP/23.1 of LA FOIP).

Section 24.1 of FOIP/23.1 of LA FOIP requires that a public body 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.

Section 24.1(a) of FOIP/23.1(a) of LA FOIP indicates that a public body 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.

Section 24.1(b) of FOIP/23.1(b) of LA FOIP indicates that public bodies 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; or
- 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.

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

A need-to-know is the principle that public bodies and their staff should only collect, use or disclose 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.

An unauthorized collection occurs when personal information is collected, acquired, received or obtained by any means for purposes that are not allowed under sections 25, 26, 27, 28 or 29(2) of FOIP/24, 25, 26, 27 or 28(2) of LA FOIP.

Unauthorized use refers to the use of personal information for a purpose that is not authorized under sections 27, 28 or 29(2) of FOIP/26, 27 or 28(2) of LA FOIP.

Unauthorized disclosure refers to the act of revealing, showing, providing copies, selling, giving, or relaying the content of personal information in ways that are not permitted under sections, 29 or 30 of FOIP/28 or 29 of LA FOIP.

Section 24.1(c) of FOIP/23.1(c) of LA FOIP indicates that public bodies should have education programs in place for their employees which addresses the public body's duties under FOIP/LA FOIP, safeguards the public body has established, the need-to-know and consequences for violating HIPA. The Office of the Information and Privacy Commissioner (IPC) has indicated that annual training is best practice.

THERE'S BEEN A PRIVACY BREACH – NOW WHAT?

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

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

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.

Notification

The following is a list of individuals or organizations that may need to be notified in the event of a privacy breach:

- Contact your organization's privacy officer immediately.
- Proactively report the breach to the IPC. For more information see the specific section on proactively reporting breaches later in this document.
- If criminal activity is suspected (e.g. burglary), contact police.
- Contact the affected individuals unless there are compelling reasons why this should not occur.

It is important to note that an amendment, effective January 2018, made to FOIP/LA FOIP in 2017 added a requirement that, if there is an unauthorized use or disclosure of personal health information, the public body must notify the affected individual if the "incident creates a real risk of significant harm" to the affected individual. See section 29.1 of FOIP/28.1 of LA FOIP.

What is a real risk of significant harm? For one, there must be some risk of damage, detriment or injury to the individual that is significant in nature. In terms of PIPEDA amendments not yet in force, "significant harm" is described as follows:

> 10.1(7) For the purpose of this section, "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 or not 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. 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?

So, does this mean that public bodies only need to provide breach notification in these cases? Not at all. A public body needs to make that call in the course of investigating any privacy breach. And, in terms of whether or not to report to the IPC, this is always encouraged. Generally, if proactively reported, this office will monitor the response to the incident by the public body and if issues are sufficiently addressed may resolve the matter informally.

It is best practice to inform affected individuals and the Information and Privacy Commissioner's office of breaches in most cases.

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.).

- 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, how to change a health services number or driver's license number etc.).
- 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 these 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?

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 a privacy breach investigation report. The report should include the following:

- A 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.
- A description of the investigative process.
- The root and contributing causes of the incident.
- A review of applicable legislation, safeguards, policies and procedures.
- A summary of possible solutions and recommendations for preventing future breaches. This should include specific timelines and responsibility for implementation of each action.

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. Gather relevant materials.
- 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 logs 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 public body to share any discipline measures taken against an employee who has snooped (without revealing the identity of the individual) 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 could come to the IPC with a complaint about a public body's actions or practices.
- A third party in possession of personal information could notify the IPC.
- Employees of a public body could inform the IPC of inappropriate practices within the organization.
- The IPC could act on media reports.
- The public body can proactively report a breach to the IPC.

What Happens When a Public Body Proactively Reports a breach to the IPC?

Public bodies should consider proactively reporting privacy breaches to the IPC. This means that when a public body learns of a breach, it reports it to the IPC. While not mandatory, the IPC does encourage organizations to proactively report.

Advantages of Proactively Reporting

Some of the benefits of proactively reporting include:

- Receiving timely, expert advice from the IPC. The IPC can help guide the public body on what to consider, what questions to ask and what parts of the legislation may be applicable.
- Should the media get wind of the privacy breach, the public body can assure the public that it is working with the IPC to address the matter.
- If satisfied with your organization's internal investigation report the IPC may close the file informally rather than issuing a public report.
- Should affected individuals contact the IPC, it can assure the individuals that it is 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 public body proactively reports a privacy breach to the IPC, a file will be opened. The public body will be asked to provide its investigation report and other material within 14 days.

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 public body'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 the Commissioner is satisfied with the public body's overall response to the breach, but the breach is egregious 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 public body'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 Commissioner is not satisfied with the public body's response, the IPC will issue a report.

Once the IPC has made a decision, the public body will be advised if a report will be issued or not. The public body will also be notified if an affected individual makes a formal complaint which would also result in a formal report.

Summary of Investigation Process

1. A privacy complaint is received at the IPC or a public body proactively reports a breach to the IPC. It will be assigned to an Early Resolution Officer (ERO).

2. ERO will ensure all necessary information has been received from the complainant, public body, or other parties. When there is a Complainant, the ERO will attempt informal resolution between the parties.

3. If early resolution is not possible, the ERO will send out a notification e-mail to all parties. It will request that an internal investigation report and relevant materials be provided in 14 calendar days. This can include:

    a. details regarding the matter,
    b. which section of applicable legislation the public body relied on for the collection, use and/or disclosure of the information in question (if relevant),
    c. details regarding how the public body took into consideration the 'data minimization' and the 'need-to-know' principles when the information in question was collected, used and/or disclosed (if relevant),
    d. 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, and
    e. a copy of public body's internal investigation report.

4. File will be assigned to an analyst. The analyst will ensure materials arrive in 14 calendar days. If materials are not received in 14 calendar days, or an agreed upon deadline, the escalation guidelines are as follows:
    a. The analyst will follow up and attempt to receive materials
    b. The analyst will escalate to the Director of Compliance (DoC) – DoC will attempt to get materials within seven calendar days before moving it on;
    c. DoC will escalate to the Commissioner - the Commissioner may contact the 'head'.

5. The analyst will review materials received – do some initial analysis to determine direction of investigation.

6. The analyst will meet with the Commissioner and DoC to discuss direction of investigation. The Commissioner may direct the Analyst to try and reach informal resolution if a complainant is not involved. If successful, file will be closed informally, without a report. Otherwise, the Analyst will prepare the draft report.

    If it is a proactively reported breach, the analyst will review materials received and meet with the Commissioner and DoC to discuss direction of investigation. The possible outcomes are as follows:

a. If the Commissioner is satisfied with the public body'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.
b. If the Commissioner is satisfied with the public body's overall response to the breach, but the breach is egregious or it involves a large number of affected individuals, the IPC may determine that a report will be issued.
c. If the Commissioner is satisfied with the public body's overall response to the breach, but an affected individual makes a formal complaint, the IPC may determine that a report will be issued.
d. If the Commissioner is not satisfied with the public body's response, the IPC will issue a report

If the IPC decides to close the file informally, the analyst will notify the public body. Otherwise, the analyst will notify the public body if the IPC has decided to issue a report.

7. The analyst will prepare a draft report. The analyst will send a PDF copy of the Draft Report to the Privacy Officer of the public body and request response within seven calendar days. The public body will be asked if there are any factual inaccuracies. This has the potential to change a finding or recommendation.

8. The analyst will put draft Report into final format and send to the Commissioner for final approval.

9. The Analyst will e-mail final report to any complainant(s) and public body.
    a. One copy of the final report will go to the complainant(s).
    b. Another copy of the final report will be e-mailed to the public body:
        i. E-mail will be sent to the Head;
        ii. E-mails will be copied to the Privacy Officer;
        iii. Additionally, copies of the final report will be sent to the Deputy Minister of Justice and other relevant Deputy Ministers.
    c. Report is now issued.

10. All reports will be posted to the website within three to five days of issuance.

11. Amendments made to sections 49 and 55 of FOIP/38 or 44 of FOIP, effective January 1, 2018, will have the effect of requiring a public body to respond to the Commissioner's final report within 30 days. It must also provide a copy of its response to any complaint(s). Pursuant to section 56 of FOIP/45 of LA FOIP, the response must be sent within 30 days of the issuance of the report. If no response is received from the public body within 23 days of issuing the final report, the analyst will provide the public body with one reminder of its duty to respond. Public body responses are tracked by the IPC.

12. Public bodies should also be aware that, because of the amendments described above, a complainant can appeal the public body's decision to the Court of Queen's Bench.

Informal Resolution

Where possible, the IPC will aim to achieve informal resolution for investigation files. Informal resolution is beneficial to all parties involved as it can expedite resolution for the Complainant and reduce the amount of work for both the public body and IPC.

When a privacy complaint is first received by the IPC, it will receive a file number and be assigned to an ERO. The ERO will first verify that the IPC had received all the necessary information and documents from the Complainant. The ERO will then contact both the Complainant and the public body in order to facilitate a possible informal resolution.

Some of the ways an ERO might facilitate an informal resolution are as follows:

- Dispel any misunderstandings.
- Clarify the applicant's objectives with the public body.
- Facilitate negotiations between the Complainant and public body.
- Clarify the role of the IPC.
- Identify the possible outcomes of an investigation.

If an ERO is not able to reach an informal resolution within a week, notification letters 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 public body's internal investigation report, we may close the file rather than conducting a formal investigation.

When informal resolution is achieved, the Commissioner will not issue a Report.

What Will be the IPC's Focus?

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

- Did the public body 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? Were they effective?;
- Training of the employees involved; and
- Potential employee snooping (if applicable).

The key questions for a privacy breach investigation can be found in this document. They capture 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 public body 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.

Draft Report

Once finished, the analyst will present a draft report to the public body which includes analysis of the file, findings and recommendations.

The public body can respond to the draft report indicating if there are any factual inaccuracies.

If a public body cannot respond within seven calendar days, please call the analyst to discuss. If there is no response, the Analyst will move the investigation forward to a final report.

Please note that the Commissioner may paraphrase or quote from a public body or complainant's submission, letter or e-mails in the draft or final report.

Commissioner's Report

Once an Analyst has received the response to the draft report from the public body, he/she will make final changes to the report and pass it to the Commissioner for his final approval.

The Commissioner will issue a report for every investigation file that is not resolved informally. A copy of the investigation report will 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 Urban Municipalities Association.

All reports will be posted on the IPC website within three to five days from issuance.

We ask that the public body provide a response to the report and recommendations within 30 days to the relevant parties.

The IPC is Paperless

The IPC has gone paperless. As such we prefer to receive correspondence, internal investigation reports and other documentation electronically. Any documentation could be sent by e-mail or by mail on a CD or USB key.

Please password protect any sensitive PDF or Word documents, especially if they contain personal information. Please do not hesitate to contact us if you require support.

Finally, please do not transmit the password in the same e-mail as the documents. Please send it in a separate e-mail or call the IPC.

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

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