PRIVACY BREACH MANAGEMENT GUIDELINES

Ministry of Justice
Access and Privacy Branch

December 2015

Government of Saskatchewan

PRIVACY BREACH MANAGEMENT GUIDELINES

Table of Contents

December 2015

Introduction

Government institutions must ensure compliance with *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Health Information Protection Act* (HIPA). Local authorities using this guide must consider *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP). All government institutions have legal and policy obligations to protect personal information and personal health information in their possession and control.

Personal information is defined in section 24 of FOIP. Among other things, it includes name, address, email address, phone number, personal opinions, financial details, and any other information which can be used to identify the individual. Personal health information is defined in section 2(m) of HIPA. It includes, among other things, any information regarding an individual's physical or mental health, services provided for their health, registration information or information collected in the course of or incidentally to the provision of health services for that individual.

If an incident occurs that puts personal information at risk, government institutions must act quickly to address the situation in a manner that will:

- Contain the problem;
- Investigate the incident;
- Ensure notifications are provided, as necessary; and
- Result in steps being taken to reduce the likelihood of the same or similar incident reoccurring.

These guidelines can be modified as necessary to suit the purposes of each government institution.

Additional information on access and privacy management is available from:

Access and Privacy Branch
Ministry of Justice
Room 520—1874 Scarth Street
REGINA SK S4P 4B3
(306) 787-5473
www.saskatchewan.ca
AccessPrivacyJustice@gov.sk.ca

Government of Saskatchewan

PRIVACY BREACH MANAGEMENT GUIDELINES

What is a Privacy Breach?

A privacy breach occurs when there is unauthorized collection, use or disclosure of personal information and/or personal health information (hereinafter collectively referred to as "personal information"). Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation.

A privacy breach may come to the attention of a government institution through its staff, the public, the Office of the Information and Privacy Commissioner (OIPC) or elsewhere.

Privacy breaches may be accidental or result from intentional actions. A privacy breach may be a one-time occurrence or may be the result of systemic issues.

The following are examples of situations that could lead to a privacy breach:

- Personal information is e-mailed or faxed to the wrong person;
- Insufficient safeguards are applied to records containing personal information (e.g. records left in an open area);
- Equipment containing personal information or personal health information is lost or stolen;
- Appropriate record disposal practices are not in place.

In these and other situations, the following guidelines can be used to determine the seriousness of the incident (e.g. conclude if a privacy breach has occurred), contain any harms and, as necessary, change practices to avoid a similar occurrence from happening.

Preventing Privacy Breaches

Protection of personal information is essential for government institutions. It is necessary for the proper conduct of the government's business process, it is critical to ensure ongoing public confidence in programs and services and it is a requirement of applicable access and privacy legislation.

Compliance with FOIP and HIPA will help protect personal information held in government institutions. However, legislative compliance alone may not be enough to ensure an effective organizational approach to privacy protection. Effective privacy management requires leadership and cooperation throughout the organization, from senior executive and managers to front line staff. In particular, government institutions should:

- Ensure lines of accountability for privacy are defined and understood. For example:
  - ◊ Appoint a Privacy Officer for the government institution and ensure proper delegation of authority under FOIP and/or HIPA is in place;
  - ◊ Place the authority for privacy breach responses with the Privacy Officer;
  - ◊ Make sure that all staff and management understand the role of the Privacy Officer.
- Develop a policy/protocol for reporting alleged privacy breaches.
- Update policies throughout the government institution to ensure there is appropriate collection, use and disclosure of personal information. For example, develop a policy respecting the collection of personal information which ensures that the legislative authority for the collection exists and the purpose for

collection is understood.

- Have administrative, technical and physical safeguards in place to protect personal Information.
- Follow proper retention schedules and ensure secure disposal of records.
- Where personal information is involved, ensure contracts with all third party service providers are in place, are consistent with the *Personal Information Contract Checklist* (available from the Access and Privacy Branch) and that they include provisions requiring the third party to report any potential privacy incidents and are required to cooperate with the government institution in privacy investigations and audits.
- Conduct a privacy review, such as a Privacy Impact Assessment, early in the development of any new initiatives (e.g. polices, programs or applications).
- Ensure the public can access their personal information and request a correction of errors in their personal information.
- Ensure that staff and the public know where to direct concerns and questions about access and privacy.
- Provide training for management and staff on policies, safeguards, individual responsibilities, etc.

Responding to Privacy Breaches

Despite efforts at prevention, privacy breaches may occur; government institutions must be prepared to respond to them. A consistent, centralized approach to privacy breaches that has the support of the organization's executive is recommended.

When a government institution becomes aware of a privacy breach, the following steps should be followed:

Step 1—Contain the Privacy Breach

1.1 Report the Privacy Breach

Immediate Supervisor

- The person discovering the problem should notify his/her immediate supervisor and follow the specific protocols established to manage the issue for the workplace.

Privacy Officer

- The Privacy Officer for the government institution should be notified as soon as possible. He or she can provide advice and should be involved in the resulting assessments and reports.

Others

- The Privacy Officer should work with the affected area to determine who else to inform/involve.
- Depending upon the circumstances, it may be necessary to inform senior management, communications staff, legal counsel and others.
- Who to involve and when will depend upon the situation. For example, if it is determined that a privacy breach did not occur, but the conditions for a privacy breach exist, then the response may require ongoing consultation in order to develop and implement an appropriate solution. If, on the other hand, it is determined that a privacy breach has occurred (e.g. records have been stolen), staff within the government institution will be notified and other external parties may be notified in order to respond to the emergent situation.

1.2 Assess the Situation

The Privacy Officer should conduct a preliminary assessment of the incident. Working with involved staff, the Privacy Officer must determine if a privacy breach has occurred and also the severity of the incident. Among other things, the Privacy Officer should answer the following questions:

- Did an inappropriate collection, use or disclosure actually occur?
- Does personal information continue to be at risk?
- Do clients or staff continue to be concerned?
- Is the incident a violation of criminal law?

If the Privacy Officer determines that a privacy breach has not occurred, the rationale for the decision should be documented.

Where it is determined that a privacy breach has occurred, the Privacy Officer must determine who has been affected by the privacy breach and what steps can be taken to contain the privacy breach and minimize any identified risks.

A privacy breach means personal information about one or more individuals has been compromised. The Privacy Officer should determine what individuals are impacted by the privacy breach and assess the level of risk posed by the privacy breach. Consider, for example:

- What amount of personal information was disclosed?
- Was the information particularly sensitive?
- Could harm result to individuals as a result of the incident?
- Is there a risk of identity theft?
- Is there a physical risk to the person?
- Are there professional, personal, institutional, reputational or other risks to consider?

1.3 Contain the Privacy Breach

If there is ongoing risk to the compromised information (e.g. an unauthorized disclosure continues to occur), then steps must be taken to prevent any further disclosure of the personal information and/or secure and recover any personal information that has been disclosed. These steps will vary with the given circumstances of a privacy breach incident.

Step 2—Investigation and Notification

After the Privacy Officer has undertaken a preliminary assessment of the incident, an investigation and notification strategy will need to be determined. The Privacy Officer may require input from a number of areas such as legal counsel, information technology services, records/ information management and the Permanent Head's office in determining the strategy. Investigation and notification strategies will vary depending on the circumstances of the incident.

A number of factors will come into play in determining when, how and who will be notified of a breach of privacy incident. Among other things, the nature, severity and impact of the breach must all be considered when determining a notification strategy.

If the incident involves potentially criminal activity, the Privacy Officer will need to consider notifying law enforcement authorities. It may not be immediately clear if criminal activity is involved in a breach, but where criminal activity is suspected, it is generally better to raise the matter with law enforcement as soon as possible.

2.1 Internal Notification

Once the incident and risks are better understood, the Privacy Officer must consider who needs to become involved in the response to the breach of privacy.

As appropriate to the situation, senior management of an affected government institution should be briefed on all reported privacy breaches. This is particularly important for cases that might garner media attention, where the incident is significant in terms of the volume or sensitivity of information involved or where law enforcement authorities may need to be involved. When a privacy breach is reported, the Privacy Officer will need to determine who in the government institution will need to be notified. Generally this will include:

- Deputy Minister's Office, CEO, Chair or equivalent;
- Communications Branch;
- Areas of the government institution that need to be involved in fixing the problem.

Briefing materials on the breach and the response to it should be prepared by the Privacy Officer.

2.2 Notify the Individuals

The Privacy Officer should consult with senior management, communications staff, etc. to determine if and how best to notify affected individuals. This consultation should occur as soon as possible after a privacy breach is discovered.

Consider the following:

<u>When to notify</u>

The determination of when it is best to notify affected individuals should be based on the preliminary analysis of the breach carried out by the Privacy Officer. The Privacy Officer should consider the nature of the breach, the amount and type of personal information involved and the potential for harm to affected individuals. For instance, individuals should be notified where it has been determined that it is possible for them to suffer harm as a result of a privacy breach (e.g. if information is disclosed that could result in identity theft and financial or other loss to the person).

Notification may allow affected individuals to take steps to reduce potential harms caused by the breach. Immediate notification is warranted in cases where someone's health or safety is potentially at risk, or where notification might assist in either investigating the cause of the event or to help prevent further loss or negative impact. Early notification might also be needed where financial or identification information (such as a social insurance number or driver's license number) is involved.

When early notification is considered, some preliminary analysis must be undertaken prior to notification in order to be able to provide some level of detail about the breach to affected individuals.

If a criminal investigation is underway, notification may need to be coordinated with law enforcement authorities in order to not interfere with their investigation.

How to notify

How notification is provided will largely depend on the circumstances of the breach. When a breach impacts a large number of individuals, it may be most efficient to provide a general public notification of the breach online, in a news release or through other similar methods.

In other circumstances, individual notice may be more appropriate. When providing individual notice, direct contact (ideally through mail and/or phone) is the suggested approach. The same details should be provided consistently to every individual when multiple parties are being informed. The option of having written information provided should be made available to affected parties. Notes of phone calls, copies of written correspondence and information on any follow-up should be documented and included in the investigation report.

What to include in notification

Notification to affected individuals should include a factual summary of what has occurred and what is being done to address the situation. The factual summary should include the basic details of the incident including the date, the specific information involved, a general description of the circumstances of the incident and any potential risks to the individual. Affected individuals should also be advised of the steps being taken to address the privacy breach, such as what the government institution is doing to recover the information and/or minimize any potential harm and what steps are being taken to review its practices to ensure a similar incident will not occur in the future.

Tell them how to contact the government institution's Privacy Officer (or other concern-handling process) in the event they are not satisfied with the actions being taken.

Provide affected individuals with contact information for the OIPC. Inform the individual that that he/she can contact the OIPC if they are not satisfied with the government institution's response to the privacy breach.

2.3 External Notification

The Privacy Officer, in consultation with the senior executive of the government institution, will need to decide if and when to inform the OIPC. Access and privacy legislation in Saskatchewan does not require the reporting of privacy breaches to the OIPC. The OIPC, however, recommends that privacy breaches are brought to the attention of the Commissioner so that a collaborative approach can be taken to dealing with the incident.

Government institutions should be aware that even if an organization investigates a privacy breach, the Commissioner may still decide to undertake a separate investigation and make public recommendations on corrective measures. In situations where the government institution is able to resolve a privacy breach to the satisfaction of the individuals involved, an individual may return to the OIPC at a later date with some concern that has arisen as a result of the privacy breach.

The Access and Privacy Branch can provide advice to help manage the incident. Please contact the Access and Privacy Branch as necessary to determine appropriate steps, including when to notify external parties.

Note: Care should be taken when notifying individuals outside the government institution to not share personal information unless it is necessary and permitted in law.

2.4 Conduct an Investigation

Privacy breach investigations should be led by the Privacy Officer, but may require input from program management and staff, human resources, legal counsel, information technology, administration, property management (physical security), records/information management, the Permanent Head's office and others. In situations where staff actions are under examination, always involve the government institution's human resources staff.

The level of formality of an investigation will depend on the seriousness of the incident. In some instances, an informal review may be sufficient. In other circumstances, a formal investigation utilizing experienced investigators may be required. In either case, the process and outcomes of an investigation should be thoroughly documented.

Every privacy breach investigation should examine policies and processes in the government institution that may have led to the privacy breach and offer suggestions for change that may prevent potential reoccurrences of the privacy breach.

A report should be produced at the conclusion of a privacy breach investigation. The report should be shared with decision-makers, as necessary, to ensure all are informed and can act on any recommendations arising out of the investigation. The report should include the following components:

- Background and scope of the review;
- Legislative considerations;
- The methodology of the review (who conducted the review, who was interviewed, what questions were asked, what policies were considered, etc.);
- A description of what happened, including chronology of events;
- An explanation of the causes;
- Recommendations for immediate or long-term corrective actions.

Step 3—Take Steps to Prevent Similar Incidents

3.1 Implement Change

Based on the findings and recommendations of the investigation, a government institution may need to do any or all of the following:

- Revise policy and procedure;
- Improve security safeguards (administrative, technical and physical);
- Provide operational and administrative staff with additional education on privacy and security to reduce the potential of future occurrence;
- Implement other recommendations identified in the investigation and report.

3.1 Review the Implementation

After an appropriate period, review the effectiveness of the actions (such as new policies and procedures). Modify them as needed.

PRIVACY BREACH RESPONSE CHECKLIST

The following checklist can be used in conjunction with the Guidelines when responding to an alleged privacy breach

	
Step 1. Contain the privacy breach	
• Notify the Privacy Officer. Determine the need to inform others at this time (legal counsel, Permanent Head, etc.)	
• Consider ongoing risk and take steps to contain the privacy breach.	
Step 2. Investigation and notification	
• Assess the situation to determine the severity of the incident.	
• Identify the parties at risk. Consider the level of personal harm.	
• Notify additional internal parties (beyond step 1 above) as necessary.	
• Notify external parties, as necessary. May include the OIPC, police and others, depending upon the circumstances.	
• Notify the individuals, if necessary. Consider the assessment in the Privacy Breach Management Guidelines.	
• Conduct an investigation—document thoroughly and issue a report, as needed.	
Step 3. Take steps to prevent similar incidents	
• Implement change resulting from the investigation.	
• After an appropriate period of time, review the effectiveness of the changes and modify, as necessary.	
• Document the response and retain the records for follow-up.	

Government of Saskatchewan