



# PRIVACY BREACH GUIDELINES

## Purpose

The Privacy Breach Guidelines may provide some guidance to government institutions, local authorities, and health information trustees (hereinafter Organizations) in Saskatchewan when a privacy breach occurs.<sup>1</sup>

The Privacy Breach Guidelines provide Organizations with some basic education about privacy breaches and take Organizations through some decision-making steps regarding notification. These guidelines may also assist Organizations in their efforts

to contain, assess and analyze a privacy breach. The guidelines also contain some preliminary steps which can be taken to prevent the breach from occurring again.

While these guidelines were created for Organizations, we encourage contractors, information management service providers (IMSP's), non-profit organizations, and other interested parties to familiarize themselves with the content within the guidelines.<sup>2</sup>

1 While these guidelines can assist Saskatchewan Organizations that are subject to *The Freedom of Information and Protection of Privacy Act*, *The Local Authority Freedom of Information and Protection of Privacy Act*, and/or *The Health Information Protection Act*, government institutions and local authorities should also refer to the Ministry of Justice and Attorney General *Privacy Breach Management Guidelines* available online at: <http://www.justice.gov.sk.ca/PBMG>

2 Contractors and IMSP's should also refer to the OIPC pamphlet "[A Contractor's Guide to Access and Privacy in Saskatchewan](#)". It discusses the access and privacy issues for any business or non-profit organization which contracts with any public body in Saskatchewan. It is available online at: <http://www.oipc.sk.ca/webdocs/ContractorsGuide.pdf>

## TABLE OF CONTENTS

	Step 1: Contain the Breach . . . . .	3
Purpose . . . . .	Step 2: Investigate the Breach . . . . .	4
What is 'Privacy'? . . . . .	Step 3: Assess and Analyze the Breach . . . . .	5
Personal Information: It's All About Me . . . . .	Step 4: Notification: Who, When and How to Notify .	6
When Does a Privacy Breach Occur? . . . . .	Step 5: Prevention . . . . .	8
Proactively Reporting Privacy Breaches to the OIPC .	The Role of the OIPC . . . . .	8
Five Key Steps in Responding to a Privacy Breach . .	Resources . . . . .	9



## What is 'Privacy'?

Privacy has been, defined in a variety of ways, and is considered to involve several different dimensions. They include:

- Physical or bodily privacy;
- Territorial privacy;
- Privacy of communications; and
- Information privacy/data privacy.

The Privacy Breach Guidelines focus on the last dimension of privacy. Information privacy

is understood as the right of an individual to determine for him/herself when, how and to what extent he/she will share his/her 'personal information'.

For the purposes of these Guidelines privacy concerns the collection, use and disclosure of personal information in compliance with the applicable legislation.

## Personal Information: It's All About Me

Personal information (PI) and personal health information (PHI) is defined by the applicable privacy law.<sup>3</sup> Generally speaking PI/PHI is information about an identifiable individual. Typically, this office will not consider a breach of privacy to have occurred if the information involved is sufficiently de-identified, provided as statistics only, or as aggregate data.

The Office of the Information and Privacy Commissioner (OIPC) of Saskatchewan may

investigate privacy breaches that involve PI or PHI of individuals. Our authority to investigate privacy breaches is established in, and limited to the PI, and/or the PHI of individuals as defined in *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), and *The Health Information Protection Act* (HIPA).<sup>4</sup>

## When Does a Privacy Breach Occur?

A privacy breach happens when there is unauthorized collection, use or disclosure of PI or PHI. Such activity is 'unauthorized' if it occurs in contravention of FOIP, LA FOIP, or HIPA.<sup>5</sup> Examples would include 'water-cooler' conversations about client PI of which a co-worker has no professional 'need to know', or a health care professional accessing a database to check a patient's status when he or she has no professional need to know the

information.

Privacy breaches most commonly occur when PI/PHI about patients, clients/customers or employees is stolen, lost, mistakenly or purposely used or disclosed without the requisite need to know. Examples include when a computer containing PI/PHI is stolen, or when PI/PHI is mistakenly emailed or faxed to the wrong person.

---

<sup>3</sup> PI is defined at section 24 of FOIP and section 23 of LA FOIP. PHI is defined at section 2(m) of HIPA.

<sup>4</sup> Links to each of these acts can be found on the Saskatchewan OIPC homepage at: <http://www.oipc.sk.ca/>. OIPC authority to investigate is established at sections 33 and 32 of FOIP and LA FOIP respectively, and sections 42(1)(c) and 52 of HIPA.

<sup>5</sup> See Part IV of FOIP, LA FOIP and HIPA.



Privacy breaches may be accidental or intentional; they may be a one time occurrence or due to systemic inadequacies such as a faulty procedure or operational

breakdown. Privacy breaches are often predictable and with proper foresight and planning can be avoided.<sup>6</sup>

### Proactively Reporting Privacy Breaches to the OIPC

The OIPC encourages Organizations to proactively report actual or potential privacy breaches to this office. Proactive reporting to the OIPC allows this office to provide advice or guidance in responding to the incident. In our experience, Organizations that alert the OIPC to a breach and take advice from our office, in terms of dealing with that breach, may be much better prepared to respond to questions from the public, the media, MLAs, etc. The Organization could then at least announce that it has alerted the OIPC and is

following advice from our office in responding to the breach.

Generally, when Organizations proactively report, the OIPC will not immediately open an investigation file, but will monitor the situation to ensure that the response of the Organization is adequate. In those instances where the response is inadequate or not timely, OIPC may open a formal investigation case file.

### Five Key Steps in Responding to a Privacy Breach

The most important step you can take is to **respond immediately to the breach**. *Step 1: Contain the Breach*, *Step 2: Investigate the Breach* and *Step 3: Assess and Analyze the Breach and Associated Risks* should be undertaken after learning of the breach.

They should be carried out as quickly as possible. *Step 4: Notification* and *Step 5: Prevention* provide recommendations for longer-term solutions and prevention strategies.

#### Step 1: Contain the Breach

Take immediate steps to contain the breach. These steps may include:

- Stop the unauthorized practice;
- Immediately contact your Privacy Officer, FOIP Coordinator, and/or the person responsible for security in your organization who should co-ordinate the following activities;
- Recover the records;
- Shut down the system that was breached;
- Revoke access or correct weaknesses in physical security; and
- Contact the police if the breach involves theft or other criminal activity, and contact affected individuals, if they may need to take further steps to mitigate or avoid further harm.

---

<sup>6</sup> An excellent tool for preventing privacy breaches is a Privacy Impact Assessment (PIA). A PIA is a diagnostic tool designed to help Organizations assess their compliance with the privacy requirements of Saskatchewan legislation. More information on PIA's can be found on our website under the heading [Privacy Impact Assessment \(PIA\)](http://www.oipc.sk.ca/resources.htm) at: <http://www.oipc.sk.ca/resources.htm>



## Step 2: Investigate the Breach

Once the breach has been contained an Organization should conduct an internal investigation. This investigation should be conducted by the Privacy Officer, FOIP Coordinator or an individual designated by the head of the Organization to conduct the investigation (hereinafter Privacy Officer). It may be conducted on an informal or formal basis depending on the nature of the breach. A breach investigation should address the incident on a systemic basis.

An internal investigation should include the following elements:

- Individuals with information about the breach should document details of the privacy breach and provide them to the Privacy Officer as quickly as possible.
- Evaluate the immediate and ongoing risks.
- Inventory and review safeguards in place prior to incident.
- Findings and recommendations.
- Write report or summary, as appropriate.

The following are some questions Organizations may wish to consider asking when conducting an internal investigation:

***What were the circumstances that lead to the breach?***

***Could the incident have been avoided?***

***Was the breach accidental or intentional?***

***Is there a risk of a repeat incident?***

***What measures need to be put in place to avoid a future similar incident?***

***Will you need to prepare an internal investigation report or just a summary/memo?***

The findings of an internal investigation should be recorded in an Investigation Report. An Investigation Report should include the following:

- A summary of the incident and immediate response to contain the breach and reduce harm.
- Steps taken to contain the breach.
- Background of the incident.
  - Include timelines and a chronology of events.
  - PI/PHI involved (data elements and sensitivity of, number affected, etc).
- A description of the investigative process.
  - Include the cause of the incident (root and contributing).
- A summary of interviews held (complainant, internal, external).
- A review of safeguards and protocols.
- A summary of possible solutions and recommendations.
- A description of necessary remedial actions, including short and long-term strategies to correct the situation (staff training, rework policies/procedures, etc).
- A detailed description of what the next steps will be.
- Responsibility for implementation and monitoring, including timelines.
  - May also include the names and positions of individuals responsible for implementation.

If your Organization does not already have a standardized Incident Response Plan or Privacy Breach Protocol it may consider developing one. An Incident Response Plan or Privacy Breach Protocol may include:



- Internal reporting protocol for incidents.
- Creating an incident response team lead by the Privacy Officer who will assign responsibility and clarify roles.
- Steps for investigating and responding to reported breaches.
- Standardize reporting mechanisms.
- Breach containment and mitigation strategy.
- Communication (including media) strategy.

### Step 3: Assess and Analyze the Breach and Associated Risks

To determine what other steps are immediately necessary, assess the risks associated with the breach. Consider the following:

#### 1. Is PI/PHI involved?

- What data elements have been breached? Generally, the more sensitive the information, the higher the risk. PHI, Social Insurance Numbers, and/or financial information that could be used for identity theft are examples of sensitive information.
- What possible use is there for the information? Can the information be used for fraudulent or otherwise harmful purposes?

#### 2. What is the cause and extent of the breach?

- What is the root cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- What short-term and long-term steps have been taken to minimize the harm?
- What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- Is the information encrypted or otherwise not readily accessible?
- Is the information de-identified, statistical or aggregate only?

#### 3. How many are affected by the Breach?

- How many individuals are affected by the breach?
- Who was affected by the breach: employees, public, contractors, clients, service providers, other organizations?

#### 4. What is the foreseeable harm resulting from the Breach?

- Is there any relationship between the unauthorized recipients and the data subject?
- What harm to the individuals will result from the breach? Harm may include:
  - Security risk (e.g. physical safety)
  - Identity theft or fraud
  - Loss of business or employment opportunities
  - Hurt, humiliation, damage to reputation or relationships
- What harm could result to the Organization as a result of the breach? For example:
  - Loss of trust in the organization, public body or custodian
  - Loss of assets
  - Financial exposure
- What harm could result to the public as a result of the breach? For example:
  - Risk to public health
  - Risk to public safety



## Step 4: Notification - Who, When and How to Notify

The key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid, mitigate or address harm to an individual whose PI/PHI has been inappropriately collected, used or disclosed. Review the risk assessment to determine whether or not notification is required; document any analysis and decisions.

Organizations that collect, use or disclose PI/PHI are responsible for notifying affected individuals when a privacy breach occurs. If the breach occurs at a third party entity that has been contracted to maintain or process PI/PHI, the breach should be reported to the originating Organization, which has primary responsibility for notification.

### 1. Notifying Affected Individuals

As noted above, notification of affected individuals should occur if it is necessary to avoid, mitigate or address harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- **Policy requires notification:** Is your Organization covered by policy that requires notification of the affected individual(s)?
- **Contractual obligations require notification:** Does your Organization have a contractual obligation to notify affected individuals in the case of a breach?
- **Risk of identity theft or fraud:** How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names **in conjunction** with SINs, credit card numbers, driver's license numbers, personal health numbers, or any other information that can be used to commit

fraud by third parties.

- **Risk of physical harm:** Does the breach place any individual at risk of physical harm, stalking or harassment?
- **Risk of hurt, humiliation or damage to reputation:** This type of harm can occur when PI/PHI such as mental health records, medical records or disciplinary records are breached.
- **Risk of loss of business or employment opportunities:** Could the breach result in damage to the reputation of an individual, affecting business or employment opportunities?

### 2. When and How to Notify

**When:** Notification of individuals affected by the breach should occur as soon as possible. However, if law enforcement authorities have been contacted, those authorities should be consulted to determine whether notification should be delayed in order not to impede a criminal investigation. Ensure all such discussions are documented.

**How:** The preferred method of notification is direct (by telephone, letter or in person) to affected individuals. This method is preferred where:

- The identities of individuals are known,
- Current contact information for the affected individuals is available,
- Affected individuals require detailed information in order to properly protect themselves from the harm arising from the Breach, and/or
- Affected individuals may have difficulty understanding an indirect notification due to mental capacity, age, language, or other factors.



Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, contact information is lacking, or where a very large number of individuals are affected by the Breach such that direct notification could be impractical. Using multiple methods of notification in certain cases may be the most effective approach.

**What:** Notifications should include the following information:

- Recognize the impacts of the breach on affected individuals and consider offering an apology;
- Date of the breach;
- Description of the breach (a general description of what happened);
- Description of the breached PI/PHI (e.g. name, credit card numbers, SINS, medical records, financial information, etc.);
- The steps taken to mitigate the harm to date;
- Next steps planned and any long term plans to prevent future breaches;
- Steps the individual can take to further mitigate the risk of harm. Provide information about how individuals can protect themselves e.g. how to contact credit reporting agencies (to set up a credit watch), how to change a health services number or driver's license number;
- Contact information of an individual within the Organization who can answer questions and provide further information; and
- That individuals have a right to complain to the OIPC. Provide contact information.

### 3. Others to Contact

Regardless of what your Organization's determinations are with respect to notifications, you should consider whether the following authorities or organizations should also be informed:

- **OIPC:** proactive disclosure of a privacy breach to the OIPC may better prepare the Organization to respond to queries from MLA's, the media, and the public. The following factors are relevant in deciding when to report a breach to the OIPC:
  - The sensitivity of the PI/PHI;
  - Whether the disclosed PI/PHI could be used to commit identity theft;
  - Whether there is a reasonable chance of harm from the Breach;
  - The number of people affected by the Breach; and
  - Whether the PI/PHI was fully recovered without further disclosure, or if any further unauthorized use has been thwarted.
- Government institutions and local authorities can also contact the **Access and Privacy Branch of the Ministry of Justice and Attorney General**, for advice in regard to responding to an incident.
- **Police:** if theft or other crime is suspected
- **Insurers or others:** if required by contractual obligations
- **Professional or other regulatory bodies:** if professional or regulatory standards require notification of these bodies
- **Credit card companies and/or credit reporting agencies:** it may be necessary to work with these companies to notify individuals and mitigate the effects of fraud.



## **Step 5: Prevention**

Once the immediate steps are taken to mitigate the risks associated with the breach, take the time to thoroughly investigate the cause of the breach. This should ultimately result in a plan to avoid future breaches. This may require an audit of physical, administrative and technical safeguards. An Organization's plan should also include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

As a result of such evaluations, Organizations should develop, or improve as necessary, adequate long term safeguards against further breaches. Policies should be reviewed and updated to reflect and implement the recommendations gleaned from the investigation. Policy review and updates should occur regularly after that.

## **The Role of the OIPC**

The OIPC is not an advocate for either the complainant or Organization involved in a breach. The OIPC is an office of last resort for individuals with privacy complaints. As such the OIPC may refer complaints back to the appropriate Organization if:

- The Organization has a designate in place equipped to handle investigation of complaints.
- The complainant has not yet raised concerns with the Organization and/or given the Organization a chance to resolve the issue.

The OIPC may initiate an investigation when circumstances exist that would make it

unreasonable to refer the complainant to the Organization, or if the complainant is dissatisfied with the Organization's response. In such instances the OIPC's role is to investigate and determine if an Organization's actions were improper and resulted in a contravention of FOIP, LA FOIP and/or HIPA.

The OIPC may be able to assist you in developing, or improving existing policies and procedures for responding to privacy breaches, and ensuring steps taken comply with obligations under privacy legislation and privacy best practices. To notify the OIPC, you may contact us at:

**OFFICE OF THE SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER**

**503 – 1801 Hamilton Street  
Regina, Saskatchewan  
S4P 4B4**

**Telephone: (306) 787-8350 / Toll Free: 1-877-748-2298  
Fax: (306) 798-1603  
E-mail: [webmaster@oipc.sk.ca](mailto:webmaster@oipc.sk.ca)**

**Website: [www.oipc.sk.ca](http://www.oipc.sk.ca)**



## Resources

The following are some excellent resources which provide more information on what to do when a privacy breach occurs, and how to help prevent security breaches.

### Access and Privacy Branch, Saskatchewan Ministry of Justice & Attorney General

- *Privacy Breach Management Guidelines*. Available online: <http://www.justice.gov.sk.ca/PBMG>
- *Help with FOIP - Privacy Compliance Checklist - Organizational Privacy Measures*. Available online: <http://www.justice.gov.sk.ca/PCCOPM>
- *Help with FOIP - Privacy Compliance Checklist - Personal Information Holdings*. Available online: <http://www.justice.gov.sk.ca/PCCPIH>

### Office of the Privacy Commissioner of Canada

- *Privacy Breach Checklist*. Available online: [http://www.privcom.gc.ca/information/guide/2007/gl\\_070801\\_checklist\\_e.pdf](http://www.privcom.gc.ca/information/guide/2007/gl_070801_checklist_e.pdf)

### Information and Privacy Commissioner/Ontario

- *Privacy Complaint Form*. Available online: [http://www.ipc.on.ca/images/Resources/up-2cmpfrm\\_e.pdf](http://www.ipc.on.ca/images/Resources/up-2cmpfrm_e.pdf)
- *What to do When Faced with a Privacy Breach: Guidelines for the Health Sector*. Available online: <http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf>

### Ombudsman Manitoba

- *Practice Note: Reporting a Privacy Breach to Manitoba Ombudsman*. Available online: <http://www.ombudsman.mb.ca/pdf/PN11b%20Reporting%20a%20Privacy%20Breach%20to%20Manitoba%20Ombudsman.pdf>

### Office of the Information and Privacy Commissioner for British Columbia

- *Privacy Breach Reporting Form*. Available online: [http://www.oipcbc.org/forms/Privacy\\_Breach\\_Form\\_\(Dec\\_2006\).pdf](http://www.oipcbc.org/forms/Privacy_Breach_Form_(Dec_2006).pdf)
- *Key Steps in Responding to Privacy Breaches*. Available online: [http://www.oipcbc.org/pdfs/Policy/Key\\_Steps\\_Privacy\\_Breaches\(June2008\).pdf](http://www.oipcbc.org/pdfs/Policy/Key_Steps_Privacy_Breaches(June2008).pdf)
- *Breach Notification Assessment Tool*. (joint project with IPC/Ontario) Available online: [http://www.oipcbc.org/pdfs/Policy/ipc\\_bc\\_ont\\_breach.pdf](http://www.oipcbc.org/pdfs/Policy/ipc_bc_ont_breach.pdf)



### Office of the Information and Privacy Commissioner of Alberta

- *Reporting a Privacy Breach to the Office of the Information and Privacy Commissioner of Alberta.* Available online: <http://www.oipc.ab.ca/ims/client/upload/Reporting%20Privacy%20Breaches%20to%20OIPC%202007.pdf>
- *Key Steps in Responding to Privacy Breaches.* Available online: <http://www.oipc.ab.ca/ims/client/upload/Key%20Steps%20in%20Responding%20to%20a%20Privacy%20Breach%202007.pdf>

### Treasury Board of Canada Secretariat

- *Guidelines for Privacy Breaches.* Available online: <http://www.tbs-sct.gc.ca/atip-ai/prp/in-ai/in-ai2007/breach-atteint-eng.asp>

This document is for general information only. It is not intended to be, and cannot be relied upon as legal advice or other advice. Its contents do not fetter, bind or otherwise constitute a decision or finding by the Office of the Information and Privacy Commissioner (OIPC) with respect to any matter, including any complaint, investigation or other matter, respecting which the OIPC will keep an open mind. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each government institution, local authority, trustee or organization.