Privacy Breach Guidelines

for Trustees

This document has two purposes. The first is to assist health trustees 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).

November 2016

Office of the
Saskatchewan Information
and Privacy Commissioner

Privacy Breach Guidelines

The Health Information Protection Act (HIPA) outlines the privacy rules for trustees. This document will explain steps to respond to a privacy breach involving personal health information. For more information about HIPA in general consult the *IPC Guide to HIPA*.

Government institutions under *The Freedom of Information and Protection of Privacy Act* (FOIP) and local authorities under *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) should consult *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

What is a Privacy Breach?

What is Privacy?

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

Personal health information is defined in section 2(m) of HIPA.

When does a Privacy Breach Occur?

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

Collection: A privacy breach could occur if a trustee asks for or collects more personal health 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, personal health information is not collected directly from the individual, etc.). The rules for collection are found in sections 23, 24 and 25 of HIPA.

Use: A privacy breach could occur when personal health information already in the possession or control of the trustee is used for reasons that are not consistent with the purpose for which they were collected (e.g. personal health information is collected to provide one service and then used to promote a different service). The rules for use are found in sections 23, 26, 29 and 30 of HIPA.

Disclosure: A privacy breach could occur when an unauthorized disclosure of personal health information transpires (e.g. when personal health information is missing, when an employee accesses personal health information without a need-to-know, when a trustee shares personal health information with another organization, etc.). Note: if personal health information in the possession or control of a trustee is missing, even if there is no evidence that someone has viewed the personal health information, it qualifies as a disclosure. The rules for disclosure are found in sections 23, 27, 28, 29 and 30 of HIPA.

Accuracy: Trustees have a duty to ensure personal health information is as accurate and complete as possible. A privacy breach may occur when personal health information is inaccurate. See section 19 of HIPA.

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.

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 health 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 health 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 indivuals unless there are compelling reasons why this should not occur.

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 health information involved (e.g. name, medical record, 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 change a health services number).
- 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 health 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?

- 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?
- 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 health 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 health 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 health 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, e-Health Saskatchewan 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 trustee 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?

The IPC can learn of a privacy breach and begin an investigation in several different ways. Some of them include:

- The trustee can proactively report a breach to the IPC.
- A citizen could come to the IPC with a complaint about a trustee's actions or practices.
- A third party in possession of personal health information could notify the IPC.
- Employees of a trustee could inform the IPC of inappropriate practices within the organization.
- The IPC could act on media reports.

What are the advantages of proactively reporting a breach to the IPC?

While not mandatory, the IPC does encourage organizations to proactively report. Some of the benefits include:

- Timely, expert advice.
- The IPC will monitor the situation and, if satisfied with your organization's internal investigation report, may close the file rather than conducting a formal investigation.
- 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 investigation by the IPC.
- Should the media get wind of the privacy breach, your organization can assure the public that they are working with the IPC to address the matter.

Summary of Investigation Process

Our goal is to complete review and investigation files on average within 33 days, 80% of the time.

1. A privacy complaint or proactively reported breach is received at the office of the Information and Privacy Commissioner (IPC). It will be assigned to an Early Resolution Officer (ERO).

2. ERO will ensure all necessary information has been received from the complainant and 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 all submissions and materials be provided in 14 days. File will be assigned to an Analyst.

4. Analyst will ensure materials arrive in 14 days.

    a. If materials are not received in 14 days, or an agreed upon deadline, the escalation guidelines are as follows:

        i. Analyst will follow up and attempt to receive materials

        ii. Analyst will escalate to Director of Compliance (DOC) – DOC will attempt to get materials within a week before moving it on;

        iii. DOC will escalate to Commissioner – Commissioner will contact the 'head'

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

6. Analyst will meet with Commissioner and DOC to discuss direction of investigation. Analyst will prepare the draft report.

7. Analyst will send PDF of Draft Report to the Privacy Officer of the trsutee (password protected) and request response in one week. The public body can contact Analyst within the one week timeframe to discuss the findings and recommendations. This has the potential to change a finding or recommendation.

8. Analyst will put draft Report into final format and send to Commissioner for final approval.

9. Analyst will e-mail Final to complainant and public body.

    a. One e-mail will go to the complainant.

    b. Another e-mail should go to the trustee:

        i. E-mail will be sent to the Head;

        ii. E-mails will be copied to the Privacy Officer, the Deputy Minister of Justice and Executive Director of the Access and Privacy Branch;

iii. Additionally, the Deputy Minister of Health should be copied on HIPA related Reports.

c. Another e-mail should go to relevant third parties if applicable.

d. Report is now issued.

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

11. If no response is received from the trustee within 30 days of issuing the final report, Analyst will provide the public body with one reminder of its duty to respond. No response is tracked as no compliance.

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 trustee 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 trustee 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 trustee.
- Facilitate negotiations between the Complainant and trustee.
- 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 trustee'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:

- 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.
- Potential employee snooping (if applicable).

The key questions for a privacy breach investigation found in this document 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 trustee 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 health information in question, etc.

Draft Report

Once finished, the Analyst will present a draft report to the trustee which includes analysis of the file, findings and recommendations.

The trustee can respond to the draft report indicating if it agrees with the findings and whether it will follow the recommendations. Please provide any final information at this time.

Again, in order to meet our goal of resolving investigation files in 33 days, 80% of the time, we ask for a response from trustees within one week. If you cannot do it in one week, 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 trustee 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 trustee, 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 report will also be sent to the Ministry of Justice and Ministry of Health.

All reports will be posted on the IPC website after three days from issuance.

We ask that the trustee 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 health 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 the IPC at 1.877.748.2298 or 306.787.8350 or by writing to:

Saskatchewan Information and Privacy Commissioner
503 – 1801 Hamilton Street
Regina, Saskatchewan
S4P 4B4

Check out our website at www.oipc.sk.ca