PRIVACY BREACH GUIDELINES

for Trustees

This document has two purposes. The first is to assist trustees as defined by *The Health Information Protection Act* 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 by the office of the Information and Privacy Commissioner (IPC). For more information, please see Part 5 and Part 7 of *The Rules of Procedure*.

Office of the
Saskatchewan Information
and Privacy Commissioner

August 2022

Contents

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 the protection of personal health information.

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 occurs when a trustee collects personal health information without authority. The rules for collection are found in sections 23, 24 and 25 of HIPA.

Use: A privacy breach occurs when personal health information, already in the possession or control of the trustee, is used without authority. The rules for use are found in sections 23, 26, 29 and 30 of HIPA.

Disclosure: A privacy breach occurs when an unauthorized disclosure of personal health information transpires (e.g., when personal health information is missing, or when a trustee shares personal health information with another organization without authority, etc.). Note: if personal health information in the custody 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.

For more on the rules for collection, use or disclosure, see *The Health Information Protection Regulations*.

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.

Duty to protect

Section 16 of HIPA requires that a trustee have administrative, technical and physical safeguards to protect personal health information.

Administrative safeguards are controls that focus on internal organization, policies, procedures and maintenance of security measures that protect personal health 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 health 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 health 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.

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.

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 health information that they do not need-to-know, either by accident or on purpose. This could also qualify as either an unauthorized use or unauthorized disclosure.

Unauthorized collection occurs when personal health information is collected, acquired, received or obtained by any means for purposes that are not authorized by HIPA.

Unauthorized use refers to the use of personal health information for a purpose that is not authorized by HIPA.

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

Trustees should have orientation and annual privacy training in place for their employees which address the trustee's duties under HIPA, safeguards the trustee has established, the need-to-know and consequences for violating HIPA.

THERE'S BEEN A PRIVACY BREACH: NOW WHAT?

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

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

Contain the breach

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

It is best practice to inform affected individuals and the IPC of breaches. The following is a list of individuals or organizations that may need to be notified as soon as possible after learning of the incident:

- Your organization's privacy officer
- The IPC (for more information see the specific section on proactively reporting to the IPC later in this document)
- The police, if criminal activity is suspected (e.g., burglary)
- The affected individuals (unless there are compelling reasons why this should not occur)

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.).
- A description of possible types of harm that may come to them as a result of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves.
- 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, including policies and procedures, were in place at the time of the privacy breach?
- Was the duty to protect met?
  - Were the safeguards followed?
  - If no safeguards were in place, why not?
  - Were the individuals involved aware of the safeguards?
- 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, health insurance 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:

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

The IPC will also request that public bodies complete the IPC's *Privacy Breach Investigation Questionnaire* (*Questionnaire*) if a file is opened. The *Questionnaire* is described later in this resource.

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
- 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 logged out of account)
- Identify and interview any witnesses
- Review the privacy training the employee in question has received (have warnings of routine audits been given?)
- Review any relevant contracts
- Consider who needs to be notified (e.g., supervisor, union, police, 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 to the rest of the employees in the organization and the affected individuals. Please also include any details of employee discipline when reporting details of the breach 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 trustee's actions or practices involving their personal health information.
- 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.
- The trustee can proactively report a breach to the IPC.

What happens when a trustee proactively reports a breach to the IPC?

Trustees should consider proactively reporting privacy breaches to the IPC. This means that when a trustee learns of a breach, it reports it to the IPC. While not mandatory, the IPC does encourage organizations to proactively report. The IPC has a reporting form for public bodies to proactively report a privacy breach to the IPC: *Proactively Reported Breach of Privacy Reporting Form for Public Bodies*.

Advantages of proactively reporting

Some of the benefits of proactively reporting include:

- May reduce the need for the IPC to issue a report on the matter
- Receive timely, expert advice from the IPC - the IPC can help guide the trustee 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 trustee can assure the public that it is working with the IPC to address the matter
- Should affected individuals contact the IPC, we can assure the individuals that 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 trustee proactively reports a privacy breach to the IPC, a file will be opened. The trustee will be asked to complete and provide the IPC's *Questionnaire* and other relevant material within 30 days.

The *Questionnaire* takes trustees through the four best practice steps of responding to a breach (containment, notification, investigation, and prevention of future breaches). Through this process of answering the questions, the completed *Questionnaire* should provide the IPC with what is required to conduct our investigation. If further information is required, the IPC will advise.

Once the IPC receives the relevant material, it will review the file and make a decision. The possible outcomes are as follows:

- If the Commissioner is satisfied with the trustee's overall response to the breach, the file will be closed informally without a public report. This process may include some informal recommendations from the IPC.
- If the breach is egregious, or it involves a large number of affected individuals, the Commissioner may determine that a report will be issued.
- If an affected individual makes a formal complaint, the Commissioner may determine that a report will be issued.

- If the Commissioner is not satisfied with the trustee's response, the IPC will issue a report.

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

Summary of investigation process

1. A privacy complaint is received by the IPC or a trustee proactively reports a breach to the IPC. It will be assigned to an Intake Officer.

2. The Intake Officer will ensure all necessary information has been received from the complainant, trustee, or other parties. When there is a complainant, the Intake Officer will attempt early resolution between the parties.

3. If early resolution is not possible, the Intake Officer will send out a notification e-mail to all parties. It will request that the *Questionnaire* and relevant materials be provided in 30 calendar days. Additional relevant materials can include copies of relevant policies and/or procedures and/or agreements (or plans to develop relevant polices and/or procedures and/or agreements) or any other relevant documentation.

4. The file will be assigned to an Analyst. The Analyst will ensure materials arrive in 30 calendar days. If materials are not received in 30 calendar days, or an agreed upon deadline, the escalation guidelines are as follows:

    - The Analyst will follow up and attempt to receive materials.
    - The Analyst will escalate to the Director of Compliance (DoC).
    - If necessary, the DoC may escalate to the Deputy Commissioner or the Commissioner, who may contact the 'head' (see section 58 of HIPA).

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

6. The Analyst will meet with the DoC, Deputy Commissioner and/or with the Commissioner to discuss the direction proposed. Informal resolution may be attempted. If successful, the file will be closed informally without a report. Otherwise, the Analyst will start working on the report.

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

- If the Commissioner is satisfied with the trustee'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 trustee's overall response to the breach, but the breach is egregious, there is a systematic issue involved, there is significant educational value or it involves a large number of affected individuals, the IPC may determine that a report will be issued.
- If the Commissioner is satisfied with the trustee'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 trustee's response, the IPC will issue a report.

If the IPC decides to close the file informally, the Analyst will notify the trustee. Otherwise, the Analyst will notify the trustee if the IPC has decided to issue a report.

7. The Analyst will draft a report and send to the Commissioner for final approval.

8. The Analyst will e-mail the final report to any complainant(s) and trustee.
   - One copy of the final report will go to the complainant(s)
   - Another copy of the final report will be e-mailed to the following:
     - Head or designate of the trustee
     - Privacy Officer
     - Deputy Minister of Health, Deputy Minister of Justice, other relevant Deputy Ministers, and any others as directed by the Commissioner

   The Report is now issued.

9. As of September 1, 2022, all reports will be posted to the website on or after seven days of issuance, unless the Commissioner directs otherwise.

10. Section 49 of HIPA requires the trustee to respond to the Commissioner's final report within 30 days. It must also provide a copy of its response to any complainant(s). The response must be sent within 30 days of the issuance of the report. Trustee responses are tracked by the IPC and reported on in the Annual Report.

11. Trustees should also be aware that a complainant may be able to appeal the trustee's decision to the Court of King's Bench (see section 50 of HIPA).

Early resolution

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

When a privacy complaint is first received by the IPC, it will receive a file number and be assigned to an Intake Officer. The Intake Officer will first verify that the IPC had received all the necessary information and documents from the complainant. The Intake Officer will then contact both the complainant and the trustee in order to facilitate a possible early resolution.

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

- Dispel any misunderstandings
- Clarify the complainant's objectives with the trustee
- Clarify the role of the IPC
- Identify the possible outcomes of an investigation

If an Intake Officer is not able to reach early resolution, 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 through informal resolution.

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:

- The duty to protect (did the trustee meet the duty to protect?)
- Compliance with the applicable legislation
- Safeguards, policies, and procedures in place at the time of the breach (were they followed and were they effective?)
- Training of the employees involved
- Potential employee snooping (if applicable)

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

Commissioner's report

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 Health, Ministry of Justice, and any other relevant ministries, organizations, or associations the Commissioner considers appropriate.

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

HIPA requires that the trustee provide a response within 30 days to the relevant parties.

CONTACT INFORMATION

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

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

503 – 1801 Hamilton Street | Regina SK S4P 4B4

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