Office of the
Saskatchewan Information
and Privacy Commissioner

Privacy Breach Investigation Questionnaire

The Privacy Breach Investigation Questionnaire (Questionnaire) is to be completed by the privacy officer or the head's/ trustee's designate for the government institution, local authority or trustee (organizations) when a breach of privacy under *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) and/or *The Health Information Protection Act* (HIPA) has occurred.

Depending on the circumstances of the breach, some of the following questions may not apply. For those questions, answer them as not applicable (NA). Please attach any relevant evidence/ documentation as appendices or send as separate attachments.

Once the Questionnaire is complete, include any relevant materials and email it to the Information and Privacy Commissioner (IPC) Analyst assigned to your file. If you would like a secure link to send the completed Questionnaire and relevant documentation to the IPC, contact the Analyst assigned to your file. If you do not wish to use a secure link, please send the Questionnaire and attachments to the Analyst in a secure fashion.

Any questions related to your investigation should be directed to the Analyst assigned to the file. If you are not sure which Analyst is assigned to the file, please call 306-787-8350 or email intake@oipc.sk.ca.

CONTACT INFORMATION

Please include the contact information of your organization's Privacy Officer or designate. In addition, please include IPC's file number and your organization's file number (if applicable). If there are others who will be assisting in this investigation (for example a law firm), please include their contact information.

Privacy Officer or Designate.....
IPC File Number.....
Organization File Number.....
Contact Information for others assisting in Investigation.....

PART I: DESCRIPTION OF THE PRIVACY BREACH

1. Provide a description of what occurred resulting in the privacy breach. The description should include whether the breach involved an inappropriate collection, use, disclosure, involves inaccurate personal information (PI) or personal health information (PHI), the organization failed to meet its duty to protect or a consent directive was not followed. In this description, please include if the privacy breach was a result of one or more of the following (check all that apply):

- ☐ Cyberattack or ransomware attack.
- ☐ Inappropriate collection of PI/PHI.
- ☐ Inappropriate use of PI/PHI.
- ☐ Inappropriate disclosure of PI/PHI.
- ☐ Employee/contractor/student snooping.
- ☐ Inaccurate PI/PHI was involved.
- ☐ Theft.
- ☐ Loss of information (e.g., briefcase left in taxi)
- ☐ Your organization otherwise failed its duty to protect PI/PHI, and if so, in what way? Example: abandoned patient records.
- ☐ Other: Please describe.

2. On what date/date range did the privacy breach occur or begin?

3. On what date was the privacy breach discovered, by whom (name and job title) and how?

4. On what date was the privacy officer notified that the privacy breach occurred and how?

5. How many affected individuals were impacted by the privacy breach? If the exact number is not known, provide an approximate number. An affected individual(s) is the individual whose PI/PHI was improperly collected, used or disclosed.

6. What PI/PHI data elements were involved or breached and is the PI/PHI involved that of employees (past or present), customers, clients or other? Be as specific as possible.

7. If you are unclear if this matter was a privacy breach and instead involved an authorized collection, use or disclosure, explain how you arrived at this conclusion. Be certain to refer to the specific authorities under FOIP, LA FOIP or HIPA (e.g., how the person had a need to know) that authorized the data transactions in question (collection, use or disclosure).

8. Is the PI/PHI involved within your possession/custody or control? Please explain how you arrived at this conclusion.

9. Please provide a copy of the organization's internal investigation report to the Analyst assigned this file by the due date in your notification email from the IPC.

PART II: STEPS TO CONTAIN THE PRIVACY BREACH

Organizations must act quickly to contain the privacy breach. This includes determining how widespread the privacy breach is, what types of PI/PHI is involved and attempting to recover the physical or electronic record or immediately stopping the unauthorized practice.

Please describe if you have or have not stopped the unauthorized practice or otherwise contained the breach. If you have not contained the breach, please indicate why.

1. If there were records involved in this privacy breach, please describe the steps you have taken to recover the records and how quickly that occurred (e.g., misdirected fax).

2. If it was a system that was breached, please describe if you were you able to shut it down and how quickly after the incident occurred and became known?

3. If an employee/contractor/student/information management service provider (IMSP) was the cause of the privacy breach, did you revoke their access to PI/PHI and if so, how quickly? Please describe. Please note that there are additional sections in this questionnaire related to breaches involving employee snooping or IMSPs.

4. If the breach was caused by a weakness in or lack of sufficient physical, technological or administrative safeguards, what steps did you take to correct the weakness or address any gaps identified?

5. If the breach was the result of a loss or theft and you were not able to contain the breach, do you still have a copy of the records that were breached?

PART III: NOTIFICATION EFFORTS

Section 29.1 of FOIP and section 28.1 of LA FOIP require that organizations take all reasonable steps to notify the affected individual(s) of an unauthorized use or disclosure of that individual's PI by the organization, if it is reasonable in the circumstances to believe that the incident created a real risk of significant harm to the individual. However, it is a best practice to notify affected individuals in all cases. Notification should happen as quickly as possible after learning of the privacy breach. If you have questions about the best way to notify affected individuals, please contact the Analyst assigned to the file.

1. Please describe how and when you notified the affected individuals of this breach and include a copy of the notification provided to the affected individuals. If notice was provided over the telephone, please provide a copy of the script that was used.

2. If you did not notify the affected individuals, please explain why not.

3. Please describe the risks to the affected individuals as a result of this privacy breach (for example are they at potential risk for identity theft, credit card fraud, humiliation, damage to reputation, etc).

4. Have the affected individuals been made aware of the risks and been offered any support or guidance to protect themselves from these risks? If yes, what was offered? For instance, did you offered the affected individual(s) protection as a result of the breach (for example, credit monitoring or fraud protection) please describe the protection offered. If you did not offer the affected individual(s) protection as a result of the breach, please describe how you assessed it was not necessary to do so.

5. If you plan on or issued a media release, please explain why you determined it was necessary and include a copy.

6. If you posted a notice of the privacy breach on your website, in a newspaper, on a social media platform (such as Facebook, Instagram, X), please provide the date posted and a copy of that notice in your office.

7. How long after learning of the breach of privacy did you report it to the IPC?

8. If you suspect criminal activity (e.g., burglary, ransomware attack), describe the circumstances.

9. If you reported this incident to the police, what police service or detachment of the RCMP was it reported to and on what date? Have the police advised they will be opening an investigation file and has a file number been assigned? If so, please provide the file number and police officer's contact information that has been assigned to the case.

10. If you determined it was necessary to notify others of this breach (for example an employee's regulatory body, union, another organization impacted by the breach), please list who you have notified and when they were notified.

PART IV: INVESTIGATE THE BREACH

1. Detail the timeline through the process of investigating the privacy breach. Please include any dates of importance and what actions occurred on those dates?

2. Where did the privacy breach occur?

3. What employees/contractors/students, if any, were involved with the privacy breach?

4. If employees/contractors/students were involved with the privacy breach, did they receive privacy training recently or ever? Please include the privacy training (content) they received and the date(s) of the privacy training.

5. If there were any witnesses to the privacy breach, please list the witnesses.

6. If you conducted interviews of employees/witnesses/others, please include a copy of the interview notes or their witness statements.

7. If you have not conducted interviews, please describe why interviews were not required.

8. What factors or circumstances contributed to the privacy breach?

9. FOIP (section 24.1), LA FOIP (section 23.1) and HIPA (section 16) impose a duty on organizations to protect PI/PHI. This duty to protect includes maintaining administrative, technical and physical safeguards to protect PI/PHI. What safeguards including policies and procedures were in place at the time of the privacy breach? Please attach copies of the relevant policies and procedures.

10. Were these safeguards, including policies and procedures, followed? Please describe how they were or were not followed?

11. Were the employees/individuals involved aware of the safeguards including policies and procedures? Please explain why or why not.

12. If no safeguards were in place to prevent this breach, please explain why not?

13. From your investigation what was the root cause or contributing cause(s)? Was the root cause of the privacy breach due to a lack of administrative, technical and/or physical safeguards or those safeguards not being following. How did you make the determination (describe)?

14. Does your organization have annual mandatory privacy training? If yes, please provide a copy of the policy, and the document employees are expected to sign when they complete the training.

IS EMPLOYEE SNOOPING INVOLVED?

Employee snooping occurs when an employee / contractor/ student/ IMSP /colleague appears to have purposely accessed PI or PHI of individuals without a legitimate need-to-know. Employee snooping can include looking up PI/PHI of themselves, their family members, friends or others for personal, not professional reasons. Is employee snooping suspected? If yes, please answer the following questions. If no, move on to Question 26 (IMSPs).

15. Please describe how the employee snooping was discovered.

16. Please explain if you did or did not suspend the snooping employee's access to PI/PHI. Why or why not?

17. If you retrieved an audit log of the snooping employee's accesses to the PI/PHI, please attach the audit logs.

18. If you did not retrieve an audit log of the snooping employee's accesses to the PI/PHI, please explain why not.

19. Did you interview the employee suspected of snooping?

20. If you interviewed the snooping employee include a copy of the interview notes or employee's statement.

21. If you did not interview the snooping employee, please explain why.

22. Please describe any employee disciplinary actions that have been taken as a result of the employee snooping.

23. Have you informed the affected individual of the name of the snooper or any disciplinary action taken? Why or why not?

24. Please describe your organization's routine auditing of employee accesses of PI/PHI on its systems.

25. If you currently do not conduct routine auditing, will you implement routine auditing as a result of this breach?

26. Please provide any other relevant information related to the employee snooping.

Please note that depending on the circumstances, my office may contact the employee in question to hear their side of the story.

IS AN IMSP OR OTHER CONTRACTOR INVOLVED?

Did this privacy breach involve a contractor or another that is providing services on your behalf? If yes, please answer the questions below. If no, move on to Part V. For the definition of an employee that includes an individual retained under contract (see subsection 2(1)(b.1) of FOIP/LA FOIP or subsection 2(1) of the HIPA Regulations) or of an IMSP (see subsection 2(1)(e.1) of FOIP/LA FOIP or subsection 2(1)(j) and section 18 of HIPA.

27. What is the nature of the relationship between the other party and your organization and what services does it provide to/on behalf of your organization?

28. Please provide a copy of the written agreement/terms and conditions/contracts with signatures, of what you have in place with the other party. If there is not a written agreement in place, please explain why.

29. What are the privacy training requirements for the other party that have access to the PI/PHI? Did they receive the required privacy training (please include date(s) and details of that training)?

30. Did you suspend the other party's access to PI/PHI? Yes or No. Please describe why you did or did not suspend the other party's access.

31. Please provide any other relevant information related to the other party's handling of this breach of privacy.

PART V: STEPS TO PREVENT FUTURE BREACHES

1. What changes are going to be made, including changes to policies and procedures, to mitigate the risk of a similar breach occurring in the future? Please indicate when you expect to make those changes.

2. What changes have been made including changes to policies and procedures? If the changes have already been made, please attach copies of the changes. If changes to policies and procedures have not been implemented yet please provide an estimated date for implementation.

3. Please describe any additional administrative, technical and/or physical safeguards that are needed as a result of this breach.

4. Please describe any additional employee training that is needed to mitigate the risks of a similar breach occurring in the future. Describe your organizations plan for this training.

5. Have you identified that a practice should be stopped related to the collection, use and/or disclosure of PI/PHI in your organization? If yes, described what steps you have taken to address this.

PART VI: ADDITIONAL INFORMATION

If there is any additional information that has not been covered above related to this privacy breach that the IPC should be made aware of, please include it here.