Office of the
Saskatchewan Information
and Privacy Commissioner

Privacy Breach Investigation Questionnaire

This questionnaire is to be completed by the privacy officer for the government institution, local authority or trustee (public bodies) once it has completed its internal investigation of 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) or *The Health Information Protection Act* (HIPA).

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

Once the questionnaire is complete, include any relevant materials and email it to the IPC Analyst assigned to your file. The IPC can now offer use of our Liquid Files, file transfer system, as a means to securely deposit large and/or sensitive documents. If you would like to provide the questionnaire and attachments using Liquid Files, please contact the Analyst and they will provide you with a file deposit link. If you do not wish to use Liquid Files, please ensure the questionnaire and attachments are provided 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 webmaster@oipc.sk.ca.

CONTACT INFORMATION

Please include the contact information of your organization's Privacy Officer. In addition, please include IPC's file number and your organization's file number (if applicable).

PART I: DESCRIPTION OF THE PRIVACY BREACH

1. Provide a description of the privacy breach. The description should include whether the breach involved an inappropriate collection, use, disclosure, involves inaccurate personal information or personal health information and/or the public body failed to meet its duty to protect.

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

3. On what date was the privacy breach discovered?

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?

6. Have you concluded that this matter was an authorized collection, use or disclosure? Yes or No? If yes, please refer to the specific authorities under FOIP, LA FOIP and/or HIPA for the authorized collection, use or disclosure. In addition, please provide an explanation as to how you concluded this was an authorized practice (e.g. how the person had a need-to-know).

7. Have you or will you be preparing an internal privacy breach report on this matter? Yes or No.

PART II: STEPS TO CONTAIN THE PRIVACY BREACH

Public bodies must act quickly to contain the privacy breach. This includes determining how broad 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.

1. Were you able to stop the unauthorized practice? Yes or No. Please describe.

2. If there were records involved in this privacy breach, were you able to recover the records and how quickly? Yes or no. If no, describe the steps you took to try and recover the records.

3. If it was a system that was breached, were you able to shut it down and if so, how quickly? Yes or No. Please describe.

4. If an employee/information management service provider (IMSP) was the cause of the privacy breach, did you revoke their access to personal information (PI)/personal health information (PHI)? Yes or No. Please describe. Please note that there are additional sections in this questionnaire related to breaches involving employee snooping or IMSPs.

5. Was this breach caused by a weakness in physical, technological or administrative safeguards? Yes or No. If yes, describe if you have or how you will correct the weakness.

PART III: NOTIFICATION EFFORTS

Section 29.1 of FOIP and section 28.1 of LA FOIP require that public bodies take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the public body 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 even if there is not a risk of significant harm. 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 IPC.

1. Did you notify the affected individuals? Yes or no. Please describe how and when you notified the affected individuals and include a copy of the notification provided to the affected individuals?

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)? If so, have the affected individuals been made aware of the risks and been offered any support or guidance to protect themselves from these risks?

4. Did you issue a media release about this privacy breach? Yes or no. If yes, please describe why you issued a media release and include a copy of it.

5. Did you post a notice of the privacy breach on your website? If yes, please provide a copy of that notice.

6. Did you place an advertisement in a newspaper regarding the privacy breach? If yes, please provide the name of the newspaper, the dates of publication and a copy of the ad.

7. Did you place a notice on any other platform (Facebook, Instagram, Twitter) of the privacy breach? If yes, please provide the name of the platform, the date and copy of the notice.

8. Did you report this breach to the IPC? If yes, on what date?

9. Do you suspect criminal activity (e.g. burglary, ransomware attack)? Yes or No. If yes, describe the circumstances.

10. Did you report this incident to the police? If so, 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.

11. Did you notify others (for example an employee's regulatory body, union, another public body impacted by the breach)? If yes, please list who was contacted and why.

PART IV: INVESTIGATE THE BREACH

1. How did you learn of the privacy breach?

2. Did you commence an investigation? If yes, when did the investigation start and describe the steps taken.

3. What PI / PHI data elements were involved in the privacy breach and for how many affected individuals?

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

5. Where did the privacy breach occur?

6. What employees, if any, were involved with the privacy breach?

7. If employees were involved with the privacy breach, did they receive privacy training? Please include the privacy training they received and the date(s) of the privacy training.

8. Were there any witnesses to the privacy breach? If yes, who?

9. Did you conduct interviews of employees/witnesses/others? Yes or no. If yes, please include a copy of the interview notes. If no, please describe why interviews were not required.

10. What was the root cause of the privacy breach?

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

12. 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.

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

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

15. If no safeguards or other policies or procedures were in place to prevent this breach, please explain why not?

IS EMPLOYEE SNOOPING INVOLVED?

Employee snooping occurs when an employee / contractor/ IMSP purposely accesses 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. Is employee snooping suspected? If yes, please answer the following questions. If no, move on to Question 23 (IMSPs).

16. Please describe how the employee snooping was discovered.

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

18. Did you retrieve an audit log of the employee's accesses? If yes, please attach the audit logs. If no, please describe why an audit of the access was not conducted.

19. Did you interview the employee? If yes, include a copy of the interview notes.

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

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

IS AN IMSP INVOLVED?

Did this privacy breach involve an IMSP? If yes, please answer the following questions. If no, move on to Part V.

22. What is the IMSPs relationship with your organization and what services does the IMSP provide to/on behalf of your organization?

23. Please provide a copy of the written agreement with signatures you have in place with the IMSP. If there is not a written agreement in place, please explain why.

24. What are the privacy training requirements for the IMSP/staff of the IMSP that have access to the PI /PHI? Did they receive the required privacy training (please include date(s) of that training).

25. Did you suspend the IMSP's access to PI/PHI? Yes or No. Please describe why you did or did not suspend the IMSPs access.

26. Please provide any other relevant information related to the IMSPs breach of the PI/PHI.

PART V: STEPS TO PREVENT FUTURE BREACHES

1. What changes have been made including changes to policies and procedures? If the changes have already been made, please attach copies of the changes.

2. 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.

3. What additional safeguards are needed? Please describe.

4. Is additional training needed to mitigate the risks of a similar breach occurring in the future? If so, please describe the plan for future training.

5. Should a practice be stopped related to PI/PHI? If yes, have you stopped the practice? Please describe.

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.