HEALTH INFORMATION

BREACH REPORTING FORM

This form was developed to guide clinics in gathering the required information to report a Health Information Act (HIA) breach to the Office of the Information and Privacy Commissioner of Alberta (OIPC). For more information on what constitutes an HIA breach, visit the [OIPC’s How to Report a Breach webpage](https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx).

# Custodian’s Information

1. Date of Report:

2. Custodian:

3. Address:

4. Custodian’s OIPC File #:

5. Contact information for a person who can answer the OIPC’s questions about the breach:

Name:

 Title/Position:

 Mailing address:

 Telephone:

 Email:

 Fax:

# Breach Description:

6. Date breach occurred:

7. Date breach ended:

8. Date breach was discovered:

9. Total number of individuals affected (or estimate if not yet known):

10. Was the information collected in Alberta? If yes, the number of individuals whose information was collected in Alberta (or estimate if not yet known):

11. The breach involved a (select all that apply):

[ ]  Loss of personal information or individually identifying health information.

If yes, what was the location of the breach (e.g. location/organization name and address):

[ ]  Unauthorized access of personal information or individually identifying health information.

[ ]  Unauthorized disclosure of personal information or individually identifying health information.

12. Describe the circumstances of the breach and the causes. **DO NOT** include individually identifying information**:**

13. Describe how the breach was discovered and who discovered it:

# Notice of Affected Individuals

14. Have the affected individuals been notified?

[ ]  Yes

[ ]  No

If yes, what date were the affected individuals notified?

15. Describe the form of the notice delivery (e.g. by letter, email):

16. Is a copy of the notice distributed to affected individuals attached to this form?

[ ]  Yes

[ ]  No

If no, describe the content of the notice. **DO NOT** include individually identifying information**:**

17. List all types of health information involved. **DO NOT** include individually identifying information**:**

[ ]  Patient information (Example: name, billing or financial information)

[ ]  Patient records (Example: diagnostic records, lab results or care plans)

[ ]  Loss of data (Example: lost computer/laptop, cybercrime)

[ ]  Archived data (Example: stored patient records)

[ ]  Other. Please list:

# Harm

18. Describe the possible harms that may occur as a result of the breach. **DO NOT** include individually identifying information**:**

### Clinic Harm

[ ]  Reputation loss and/or loss of clients

[ ]  Legal action

[ ]  Cybercrime

[ ]  Financial loss

[ ]  Other. Please list:

### Patient Harm

[ ]  Embarrassment

[ ]  Reputational loss

[ ]  Financial loss

[ ]  Criminal use of information (e.g. identity theft)

[ ]  Other. Please list:

# Risk Assessment

19. Provide an assessment of the likelihood that the harm will occur. **DO NOT** include individually identifying information**.**

The level of harm becomes significantly more likely based on the number of people affected, sensitivity of health information released, and mode of information release (e.g. internet, lost paper file, etc.)

**Categorize the level of risk:**

[ ]  Low

Considerations: small number of individuals affected (e.g. 1-10), sensitivity of information low (e.g. financial information), mode of release (e.g. misplaced file, released to incorrect health care organization).

[ ]  Medium

Considerations: moderate number of individuals affected (e.g. 11-50), sensitivity of information moderate (e.g. positive lab results), mode of release (e.g. information released to incorrect patient or organization, inappropriate employee access)

[ ]  High

Considerations: large number of individuals affected (e.g. 51+), sensitivity of information high (e.g. complete medical records, reputation harming content such as positive cancer or STI results), mode of release (e.g. internet, cybercrime)

**Describe the reasoning for your level of risk choice:**

# Risk Mitigation

20. Describe the steps taken to reduce the risk of harm to affected individuals:

21. Describe the steps taken to reduce the risk of a similar event occurring in the future:

# Additional Information

22. Has your privacy officer and/or person responsible for security in your organization been notified of the breach?

[ ]  Yes

[ ]  No

If yes, provide the name and contact information of the privacy officer, and the date notified.

 Name:

 Contact information (phone number and email):

 Date notified:

23. Have the police or any other authorities or organizations been notified about the breach?

[ ]  Yes

[ ]  No

If yes, provide the name and contact information for each entity notified, and the date notified:

Entity 1:

Name:

Contact information (phone number and email):

Date notified:

Entity 2:

Name:

Contact information (phone number and email):

Date notified:

24. Provide any additional relevant information regarding the privacy breach:

# Submitting to the Commissioner

Custodians are required to notify the Commissioner of a reportable breach under the *Health Information Act* as soon as practicable.

Email is the preferred method to submit: breachreport@oipc.ab.ca.

Mailing address:

Office of the Information and Privacy Commissioner of Alberta

410, 9925 - 109 Street

Edmonton, AB T5K 2J8

For general information about responding to a privacy breach, please contact the OIPC by telephone at 780-422-6860 or toll free 1-888-878-4044.

# Questions?

If you have any questions about this document or require further assistance, please contact the Alberta Medical Associations’ Security Privacy and Data Sharing (SPaDS) team at privacySPaDS@albertadoctors.org.