# Breach Documentation Form

# Document Purpose and Overview

The Health Information Act (HIA) states a privacy breach means a loss of, unauthorized access to, or unauthorized disclosure of health information.

This form is intended to guide custodians through the process of addressing a breach including determining the extent of the breach and the potential risk of harm. Please refer to your clinic’s Breach Management Policy or to the [AMA Breach Management Policy](https://www.albertadoctors.org/clinic-patient-privacy/breach-mgmt-policy.docx) guidance document from the AMA website for further information. If you need additional assistance, you may wish to contact a privacy consultant.

This form can be filled out by the privacy officer but must be signed off by the custodian. The form also serves as a record of the breach and action taken. It should be filed in a secure location to be referenced in the future if needed.

# Instructions for use

The instructions below are meant to assist you with making this document your own and to fulfill your obligations under the Health Information Act.

* This form can be filled out by the privacy officer but must be signed off by the custodian.
* The form also serves as a record of the breach and action taken. It should be filed in a secure location to be referenced in the future if needed.
* **Patient names should not be included in the information shared to OIPC or the Minister.** **This documentation is for your information only and you must fill out the appropriate reporting forms for OIPC and the Minister.**

# Privacy Training

The Alberta Medical Association offers privacy and security training to any Alberta community-based medical clinic. [Visit the AMA website today to learn more!](https://www.albertadoctors.org/leaders-partners/clinic-patient-privacy/privacy-training)

**Breach Documentation Form**

|  |
| --- |
| **Part A. Breach Information**  |
| Complete the section below to conduct a full assessment of the breach that has occurred. It is important to assess all elements of the breach as this will help you to determine the risk of harm and the need to report the breach. It’s important to include your rationale in the sections provided because you may need to refer to this information in the future. |
| Name of person filling out the form: | Date: |
| Privacy Officer informed:  | **Yes** | **No** | Privacy Officer name: |
| □ | □ |
| Key physicians involved informed:  | **Yes** | **No** | Lead clinic physician name: |
| □ | □ |
| Describe how the breach was discovered. Who were the key staff and physicians involved in the breach and what was their role? |
|  |
| Was the cause of the breach a loss of information **OR** unauthorized access **OR** unauthorized disclosure? Describe your reasoning below. |
|  |
| List the types of health information involved. Health Information includes diagnostic, treatment and care information or registration information. This pertains to #11 on the OIPC privacy breach reporting form. Do not include individually identifying information. |
|  |
| When did the breach occur? When was it discovered? |
|  |
| Whose information has been breached?  |
|  |
| If the information has been disclosed, how wide is the spread of information? Please describe below. |
|  |

|  |
| --- |
| **Part B. Risk of Harm**  |
| The Health Information Regulation defines the factors custodians must consider when assessing the risk of harm. This checklist can be used to assist the custodian and privacy officer to ensure all factors were considered.  |
| **RISK OF HARM CONSIDERATIONS** | **Yes** | **No** | **ASSESSMENT RATIONALE** |
| Is there reason to believe that the information has been or may be accessed by or disclosed to an unauthorized individual?  | □ | □ |  |
| Is there a reason to believe that the information has been or will be used for malicious purposes (intentional or not)?  | □ | □ |  |
| Is there a reason to believe that the information could be used for the purpose of identity theft or to commit fraud? | □ | □ |  |
| Is there a reason to believe that the information involved in the breach could cause:* Embarrassment
* Physical, mental, or financial harm
* Damage of reputation
 | □ | □ |  |
| Is there a reason to believe that the breach has or may adversely affect the provision of a health services to the individual? | □ | □ |  |
| Are there any other factors that indicate a risk of harm to the affected individual? | □ | □ |  |
| \*If you answer “YES” to any of the questions, please continue on to Section C to ensure that the breach was not mitigated before notice under Section 60.1(2) of the HIA. \*If you answer “NO” to all the questions then the breach may not be reportable. |

| **Part C. Mitigation Factors**  |
| --- |
| There are mitigating factors that a custodian must consider in reporting a breach. Complete the section (s) that is applicable to your type of breach. |
|  | **Yes** | **No** |
| 1. For loss of information:
 |
| * Was the electronic information encrypted or otherwise secured in a manner that would prevent the information from being accessed or make the information useless?
 | □ | □ |
| * Do you have confirmation the information was destroyed or made useless?
 | □ | □ |
| * + If it was recovered, is there confirmation that it was not accessed before it was recovered?
 | □ | □ |
| * + If it was recovered, is there confirmation that the information was only viewed to determine that the information was provided in error?
 | □ | □ |
| 1. For unauthorized access of information, can the custodian demonstrate that the person:
 |
| * Is a custodian or an affiliate?
 | □ | □ |
| * Is subject to a confidentiality agreement and HIA compliant policies and procedures?
 | □ | □ |
| * Accessed the information in a manner that is relevant to the person’s duties?
 | □ | □ |
| * Was not inappropriately accessing information? (i.e., snooping)
 | □ | □ |
| * Did not use the information except in determining that the information was accessed in error, and steps have been taken to address the error?
 | □ | □ |
| 1. For unauthorized disclosure of information, can the custodian demonstrate:
 |
| * That the information was disclosed to a custodian or an affiliate?
 | □ | □ |
| * That the recipient was subject to a confidentiality agreement and HIA compliant policies and procedures?
 | □ | □ |
| * That the person disclosing the information had the authority to do so?
 | □ | □ |
| A custodian may decide that notification is necessary even when mitigating factors are present. Each situation is unique, and all factors should be considered. |

|  |
| --- |
| **Part D. Reporting and Mitigation:** |
| The custodian must report the breach unless they are able to demonstrate the breach was mitigated and there was no risk of harm. Use the checklist below to document your reporting and attach the forms sent to the various parties.  |
| **Did the custodian report the breach?** | **Yes** | **No** | **Date (if applicable)** |
| Notified OIPC using OIPC privacy breach reporting form | □ | □ |  |
| Notified Minister of Health using AH Minister reporting form | □ | □ |  |
| Notified the patient using patient notification letter template | □ | □ |  |
| **Mitigation and Remediation Notes** |
| Describe any steps that the custodian has taken or is intending to take, to reduce the risk of harm to the individual(s) involved in this breach. |
|  |
| Describe any steps that the custodian has taken or is intending to take, to reduce the risk of future breaches.  |
|  |
| Custodian Signature: | Date: |