

## 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:	<b>Yes</b>	<b>No</b>	Privacy Officer name:
	<input type="checkbox"/>	<input type="checkbox"/>	

Key physicians involved informed:	<b>Yes</b>	<b>No</b>	Lead clinic physician name:
	<input type="checkbox"/>	<input type="checkbox"/>	

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?	<input type="checkbox"/>	<input type="checkbox"/>	
Is there a reason to believe that the information has been or will be used for malicious purposes (intentional or not)?	<input type="checkbox"/>	<input type="checkbox"/>	
Is there a reason to believe that the information could be used for the purpose of identity theft or to commit fraud?	<input type="checkbox"/>	<input type="checkbox"/>	
Is there a reason to believe that the information involved in the breach could cause: <ul style="list-style-type: none"> <li>• Embarrassment</li> <li>• Physical, mental, or financial harm</li> <li>• Damage of reputation</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	
Is there a reason to believe that the breach has or may adversely affect the provision of a health services to the individual?	<input type="checkbox"/>	<input type="checkbox"/>	
Are there any other factors that indicate a risk of harm to the affected individual?	<input type="checkbox"/>	<input type="checkbox"/>	

\*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?	<input type="checkbox"/>	<input type="checkbox"/>
• Do you have confirmation the information was destroyed or made useless?	<input type="checkbox"/>	<input type="checkbox"/>
• If it was recovered, is there confirmation that it was not accessed before it was recovered?	<input type="checkbox"/>	<input type="checkbox"/>
• If it was recovered, is there confirmation that the information was only viewed to determine that the information was provided in error?	<input type="checkbox"/>	<input type="checkbox"/>
2. For unauthorized access of information, can the custodian demonstrate that the person:		
• Is a custodian or an affiliate?	<input type="checkbox"/>	<input type="checkbox"/>
• Is subject to a confidentiality agreement and HIA compliant policies and procedures?	<input type="checkbox"/>	<input type="checkbox"/>
• Accessed the information in a manner that is relevant to the person's duties?	<input type="checkbox"/>	<input type="checkbox"/>
• Was not inappropriately accessing information? (i.e., snooping)	<input type="checkbox"/>	<input type="checkbox"/>
• Did not use the information except in determining that the information was accessed in error, and steps have been taken to address the error?	<input type="checkbox"/>	<input type="checkbox"/>
3. For unauthorized disclosure of information, can the custodian demonstrate:		
• That the information was disclosed to a custodian or an affiliate?	<input type="checkbox"/>	<input type="checkbox"/>
• That the recipient was subject to a confidentiality agreement and HIA compliant policies and procedures?	<input type="checkbox"/>	<input type="checkbox"/>
• That the person disclosing the information had the authority to do so?	<input type="checkbox"/>	<input type="checkbox"/>

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.

<b>Did the custodian report the breach?</b>	<b>Yes</b>	<b>No</b>	<b>Date (if applicable)</b>
Notified OIPC using OIPC privacy breach reporting form	<input type="checkbox"/>	<input type="checkbox"/>	
Notified Minister of Health using AH Minister reporting form	<input type="checkbox"/>	<input type="checkbox"/>	
Notified the patient using patient notification letter template	<input type="checkbox"/>	<input type="checkbox"/>	

**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:
----------------------	-------