HIA Privacy Breach Management Policy

Created Date: _____ Revision Date:_____

Applies to: All Employees, Contractors and Volunteers

Approved by:

Duty to Notify

In 2014, The Alberta Health Information Act (HIA) was amended to include section 60.1 that requires health custodians (or affiliates to custodians) to give notice, in accordance with the regulations, of a loss or any unauthorized access to, or disclosure of individually identifying health information in the custody of control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure. Pending approval for supporting regulations, the breach reporting requirements took effect on August 31, 2018.

Notification

Section 60.1 of the *Health Information Act* requires notification to the Commissioner, Minister of Health, and affected individual(s) where: (See forms at the bottom of this document)

- There has been **any loss of, or any unauthorized access to, or disclosure of** individually identifying health information; and
- There is a risk of harm to the individual who is the subject of the information as a result of the loss or unauthorized access or disclosure.

An access or disclosure is "unauthorized" if it occurs in contravention of the *Health Information Act* or its regulations.

Affiliate's Duty to Notify

Section 60.1(1) of the HIA requires an affiliate of a custodian who becomes aware of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian to, as soon as practicable, notify the custodian in accordance with the regulations.

Custodian's Duty to Notify

Subsections 60.1(2) and (3) of the HIA require a custodian to notify the Commissioner, Minister of Health, and individual who is the subject of the information of any loss of, unauthorized access to, or disclosure of individually identifying health information in the custody or control of the custodian if there is a risk of harm to the individual who is the subject of the information as a result of the loss or unauthorized access or disclosure.

Assessment of Risk of Harm

Where a custodian becomes aware of a loss or unauthorized access or disclosure, the custodian is required to assess whether there is a risk of harm to the individual who is the subject of the information as a result of the loss or unauthorized access or disclosure. If a risk of harm is determined to exist, section 60.1(2) of the Health Information Act requires the custodian to undertake notification.

Factors to Consider

Section 8.1(1) of the Health Information Regulation sets out the factors that a custodian must consider when assessing the risk of harm. A custodian is required to consider the following factors, in addition to any other relevant factors:

(a) Whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person
(b) Whether there is a reasonable basis to believe that the information has been misused or will be misused
(c) Whether there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud
(d) Whether there is a reasonable basis to believe that the information is of a type that could cause embarrassment or physical, mental, or financial harm to or damage the reputation of the individual who is the subject of the information
(e) Whether there is a reasonable basis to believe that the loss of or unauthorized access to or disclosure of the information has adversely affected or will adversely affect the provision of a health service to the individual who is the subject of the information
(f) In the case of electronic information, whether the custodian can demonstrate that the information was encrypted or otherwise secured in a manner that would:
    i. Prevent the information from being accessed by a person who is not authorized to access the information, or
    ii. Render the information unintelligible by a person who is not authorized to access the information.
(g) In the case of a loss of information, whether the custodian can demonstrate that the information was lost in circumstances in which the information was:
    i. Destroyed, or
    ii. Rendered inaccessible or unintelligible.
(h) In the case of a loss of information that is subsequently recovered by the custodian, whether the custodian can demonstrate that the information was not accessed before it was recovered.
(i) In the case of an unauthorized access to or disclosure of information, whether the custodian is able to demonstrate that the only person who accessed the information or to whom the information was disclosed:
    i. Is a custodian or an affiliate,
    ii. Is subject to confidentiality policies and procedures that meet the requirements of section 60 of the Act,
    iii. Accessed the information in a manner that is in accordance with the person's duties as a custodian or affiliate and not for an improper purpose, and

iv. Did not use or disclose the information except in determining that the information was accessed by or disclosed to the person in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure

The amending Regulation also adds sections 8.2 and 8.3 that detail provisions on the content of the required notice of a custodian to each, the Privacy Commissioner, the Minister of Health, and the affected individual.

Offence

There are several offences related to mandatory breach reporting under the HIA (sections 107(1.1) and (1.2)).

It is an offence for a custodian:

- To fail to take reasonable steps in accordance with the *HIA* Regulations to maintain administrative, technical, and physical safeguards that will protect against any reasonably anticipated threat or hazard to the security or integrity of health information or the loss of health information
- To fail to give notice of a reportable privacy breach under section 60.1(2) of the HIA to the Commissioner, the Minister of Health, and affected individuals, in accordance with section 60.1(3) of the HIA
- To fail to consider all relevant factors, including the factors prescribed by Regulations, in assessing whether there is a risk of harm to an individual for determining whether notice of a privacy breach must be given, in accordance with section 60.1(4) of the HIA
- To fail to give notice to the Commissioner of a decision not to notify an affected individual of a privacy breach in accordance with section 60.1(5) of the HIA

It is an offence for an affiliate of a custodian to fail to notify the custodian in accordance with section 60.1(1) of the HIA of a privacy breach of individually identifying health information in the custody or control of the custodian.

If guilty of an offence, fines may be applied, as per (section 107(7)) of the HIA.

References

Office of the Information and Privacy Commissioner of Alberta – Clinic Note, Reporting a Breach to the Commissioner

Health Information Act Guidelines and Clinic Manual, Chapter 14 Duty to Notify

Health Information Regulation Amendments: Mandatory Breach Notification, Continuity of Care Leaders Group June 27, 2018.

Risk of Harm Checklist

Created Date: _____ Revision Date:_____

Applies to: All Employees, Contractors, and Volunteers

Approved by:

Health Information Act (HIA)

Risk of Harm Considerations and Notification Requirements

The Health Information Act (HIA) under Section 60.1 (2) provides that a Custodian must as soon as practicable give notice for any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the Custodian if there exist a risk of harm to an individual as a result of the loss or unauthorized access or disclosure.

Further, the HIA under Section 60.1 (3) requires that notice must be given to the Information and Privacy Commissioner of Alberta (Commissioner), the Minister of Health of Alberta (Minister), and the individual who is the subject of the individually identifying health information. However, Section 60.1 (5) states that if the Custodian is aware that there would be a risk of harm to the individual's mental or physical health as a result of giving notice, the Custodian may decide not to notify the individual and must immediately give notice to the Commissioner of the decision not to notify the individual and the reason(s) for the decision.

The following questions will guide Custodians in assessing the existence of risk of harm.

What is the meaning of "as soon as practicable"?

Giving notice for any loss of individually identifying health information or any unauthorized access to or disclosure must be done as soon as practicable (able to be done or put into practice successfully) or as soon as you become aware of the loss, unauthorized access to or disclosure of individually identifying health information.

What is a loss, unauthorized access, or unauthorized disclosure?

A **loss** occurs where information, which was once in the custody or under the control of a Custodian, is no longer in the custody or under the control of that Custodian. A loss may involve physical or electronic records.

Examples of loss:

- Where a medical record is lost by a storage facility contracted by a Custodian
- Where server data becomes corrupted, resulting in a loss of digital files
- Where physical clinic files have been the subject of theft or were destroyed due to accidental fire

An **unauthorized access** occurs where an individual accesses information that they were not authorized to use or acquire any information.

Examples of unauthorized access:

- Where an electronic health record was deliberately accessed by an unauthorized individual
- Where a health professional access patients' records that are not under its direct care
- Where a health professional access the health information of a different person but with similar name

An **unauthorized disclosure** occurs where there has been a deliberate or accidental disclosure of individually identifying health information in contravention of the HIA.

Examples of unauthorized disclosure:

- Where there has been a misdirected fax or received by an unintended recipient
- Where a disclosure is made outside of the terms of a valid consent
- Where a document containing health information instead of shredding was dumped to landfill and found by waste disposal employee

What are the factors to consider in assessing risk of harm?

The Health Information Regulation sets out the factors that Custodian must consider when assessing risk of harm. The checklist below can be used to assist Custodian in ensuring all required factors will be considered to gauge the risk involve.

ITEM #	REQUIRED CONSIDERABLE FACTORS	YES	NO
1	Is there a reason to believe that the information has been or may be accessed by or disclosed to a person?		
2	Is there a reason to believe that the information has been misused or will be misused?		
3	Is there a reason to believe that the information could be used for the purpose of identity theft or to commit fraud?		
4	Is there a reason to believe that the information involved is of a type that could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual who is the subject of the information?		
5	Is there a reason to believe that the loss, unauthorized access or disclosure has adversely affected, or will adversely affect the provision of a health service to the individual who is the subject of the information?		
6	Are there any other factors that indicate a risk of harm to the individual who is the subject of the information?		

*If you answer "YES" to any of the questions in the considerable factors, the Custodian may be required to give notice under Section 60.1 (2) of the HIA. However, there are other mitigating factors that a Custodian must consider to wherein risk is appropriately mitigated and therefore notification is not required.

ITEM #	MITIGATING FACTORS	YES	NO
1	In the case of electronic information, can the Custodian demonstrate that the information was encrypted or otherwise secured in a manner that would: • prevent the information from being accessed by a person who is not authorized to access the information? Or • render the information unintelligible by a person who is not authorized to access the information?		
2	If the information was lost, can the Custodian demonstrate that the information was lost in circumstances in which the information was destroyed or rendered inaccessible?		
3	If the information was lost, and subsequently recovered by the Custodian, can the Custodian demonstrate that the information was not accessed before it was recovered?		
4	In the case of an unauthorized access to or disclosure of information, can the Custodian demonstrate that the only person who accessed the information (or to whom the information was disclosed meets all of the following requirements: • is a Custodian or an Affiliate? • is subject to confidentiality policies and procedures that meet the requirements of Section 60 of the HIA? • accessed the information in a manner that is in accordance with the person's duties as a Custodian or Affiliate and not for an improper purpose? and • did not use (or disclose) the information except in determining that the information was accessed by (or disclosed to) the person in error and in taking any steps reasonably necessary to address the unauthorized access (or disclosure)?		
5	Are there any other factors that indicate that the risk may be mitigated?		

*If you answer "YES" to any of the questions in the mitigating factors, the Custodian may appropriately mitigate the considerable risk factors and therefore notification is not required. In some circumstances, a Custodian may decide that a notification is necessary even when mitigating factors are present especially if it involves all of the foregoing considerable factors. A Custodian must consider that each situation is unique, and all factors should be considered.

What is the meaning of "reasonable basis"?

Reasonable basis exists where a Custodian can, based on its professional judgment, understanding of the incident or other relevant information such as recommendations from privacy, security, and legal terms, will commit to a decision that the factor in consideration is applicable to the situation.

What are the contents of notification to an affected individual?

The notification to an affected individual must be in writing and must include the following data elements:

- **Custodian Information**
  i. The name of the Custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure.
  ii. The name and contact information for a person who is able to answer questions or concerns about the loss or unauthorized access or disclosure on behalf of the Custodian.
- **Incident Description**
  i. A description of the circumstances of the loss or unauthorized access or disclosure.
  ii. The date on which (or period of time within which) the loss or unauthorized access or disclosure occurred.
- **Type of Information Involved**
  i. A non-identifying description of the type(s) of information that was involved in the loss, unauthorized access or disclosure (e.g., stating only diagnostic or imaging report, prescription information, Personal Health Number, etc.)
- **Risk of Harm**
  i. A non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure. Your description must not identify an individual, but should include the following information:
    a) The type of harm, and
    b) An explanation of how the risk of harm was assessed.
  ii. A description of any steps that the Custodian has taken or is intending to take, as of the date of the notice to reduce the risk of harm to the individual as a result of the loss or unauthorized access or disclosure.
  iii. A description of any steps that the Custodian has taken or is intending to take, as of the date of the notice to reduce the risk of future loss or unauthorized access or disclosure.
  iv. A description of any steps that the Custodian believes the individual may be able to take to reduce the risk of harm to the individual.
- **Additional Information**
  i. Any other information that the Custodian considers to be relevant to the affected individual.
  ii. A statement that the individual has a right to complain to or request an investigation from the Office of the Information and Privacy Commissioner (OIPC) of Alberta in regard to the loss or unauthorized access or disclosure.
  iii. Contact information for the OIPC.

What are the contents of notification to the Minister?

The notice must include the following listed information and that a Custodian must notify in writing and in a form approved by the Minister. Please email completed OIPC breach form to the following contact information for the minister of health. (See attached form)

_____

Minister of Health
Office of the Minister

Health
423 Legislature Building
10800 - 97 Avenue
Edmonton, AB
T5K 2B6

Phone: 780 427-3665
Fax: 780 415-0961
E-mail: health.minister@gov.ab.ca

- **Custodian Information**
  i. The name of the Custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure.
  ii. The name and contact information for a person who is able to answer questions or concerns about the loss or unauthorized access or disclosure on behalf of the Custodian.
- **Incident Description**
  i. A description of the circumstances of the loss or unauthorized access or disclosure.
- **Type of Information Involved**
  i. A non-identifying description of the type(s) of information that was involved in the loss, unauthorized access or disclosure (e.g. stating only diagnostic or imaging report, prescription information, Personal Health Number, etc.)
- **Risk of Harm**
  i. A non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure. Your description must not identify an individual, but should include the following information:
    a) The type of harm, and
    b) An explanation of how the risk of harm was assessed.
  ii. The exact number, or if the exact number cannot be determined, an estimate of the number of individuals to whom there is a risk of harm as a result of the loss or unauthorized access or disclosure.
  iii. A description of any steps that the Custodian has taken or is intending to take, as of the date of the notice to reduce the risk of harm to an individual as a result of the loss or unauthorized access or disclosure.
- **Additional Information**
  i. Any other information that the Custodian considers to be relevant.

What are the contents of notification to the Commissioner?

The notice must include the following listed information and that a Custodian must notify in writing and in a form approved by the Commissioner. Follow this link to fill out the OIPC Breach Reporting form in the event of a breach.

https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx

- **Custodian Information**
  i. The name of the Custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure.
  ii. The name and contact information for a person who is able to answer questions or concerns about the loss or unauthorized access or disclosure on behalf of the Custodian.
- **Incident Description**
  i. A description of the circumstances of the loss or unauthorized access or disclosure.
  ii. The date on which (or period within which) the loss or unauthorized access or disclosure occurred.
  iii. The date the loss or unauthorized access or disclosure was discovered.
- **Type of Information Involved**
  i. A non-identifying description of the type(s) of information that was involved in the loss, unauthorized access or disclosure (e.g. stating only diagnostic or imaging report, prescription information, Personal Health Number, etc.)
- **Risk of Harm**
  i. A non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure. Your description must not identify an individual, but should include the following information:
    c) The type of harm, and
    d) An explanation of how the risk of harm was assessed.
  ii. The exact number, or if the exact number cannot be determined, an estimate of the number of individuals to whom there is a risk of harm as a result of the loss or unauthorized access or disclosure.
  iii. A description of any steps that the Custodian has taken or is intending to take, as of the date of the notice to reduce the risk of harm to an individual as a result of the loss or unauthorized access or disclosure.
- **Additional Information**
  i. Any other information that the Custodian considers to be relevant.

HIA Breach Reporting Form

1. Date of Report:

2. Custodian:

3. Address:

4. Custodian 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:

Loss of personal information or individually identifying health information.

Unauthorized disclosure of personal information or individually identifying health information.

Unauthorized disclosure of personal information or individually identifying health information.

---

12. Loss of personal information or individually identifying health information

Location of the breach:

13. Describe the circumstances of the breach and the causes. Do not include individually identifying information.

14. Describe how the breach was discovered and who discovered it.

Notice of Affected Individuals

15. Have affected individuals been notified?

16. Describe the content of the notice (**do not include individually identifying information**):

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

18. Date when affected individuals were notified:

19. Copy of notice is attached. **Do not include individually identifying information:**

Health Information involved

20. List the types of health information involved. *Do not include individually identifying information.*

Harm

21. Describe the possible harms that may occur as a result of the breach. Do not include individually identifying information.

Risk Assessment

22. Provide an assessment of the likelihood that the harm will result. Do not include individually identifying information.

Risk Mitigation

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

---

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

Additional Information

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

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

Name:

Contact information:

Date notified:

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

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

Name:

Contact information:

Date notified:

27. 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 submissions are preferred. Please submit the completed Privacy Breach Report Form to breachreport@oipc.ab.ca.

If you are unable to submit the form by email, you can submit it to:

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.

Submitting to the Minister of Health

The form must also be submitted to the Minister of Health:

health.minister@gov.ab.ca

Search AMA's Resource Centre for more tools.