HEALTH INFORMATION ACT: RISK OF HARM CONSIDERATIONS AND NOTIFICATION REQUIREMENTS

Section 60.1 (2) of the Health Information Act (HIA) requires that a Custodian must 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 as soon as practicable if there is a *risk of harm* to an individual as a result of the loss or unauthorized access or disclosure.

Section 60.1 (3) of the HIA further 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) of the HIA*** 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 can decide not to notify the individual. They must immediately give notice to the Commissioner of the decision not to notify the individual and the reason(s) for the decision if they pursue this option.

The following questions may be of benefit to the Custodian in assessing whether a risk of harm exists.

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

In the context of ***Section 60.1 (1) of the HIA***, as soon as practicable means as soon as the Custodian or Affiliate becomes aware of the loss, unauthorized access or disclosure, and has gathered the relevant information necessary to properly provide the notice, they will provide the notice without delay.

II. 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 the 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

Unauthorized access occurs where an individual accesses information that they were not authorized to access.

Examples of unauthorized access:

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

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 a fax received by an unintended recipient
- Where a disclosure is made outside of the terms of a valid consent
- Where a document containing health information that was supposed to be shredded was dumped in a landfill and found by a waste disposal employee

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

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

ITEM	REQUIRED CONSIDERABLE FACTORS	YES	NO
1	Is there a reasonable basis to believe that the information has been or may be accessed by or disclosed to the incorrect person?		
2	Is there a reasonable basis to believe that the information has been misused or will be misused?		
3	Is there a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud?		
4	Is there a reasonable basis 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 reasonable basis 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, as a Custodian you may be required to give notice under ***Section 60.1 (2) of the HIA***. However, there are other mitigating factors that you must consider that may assist you in determining whether the risk was appropriately mitigated against and therefore notification may not be 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?		

ITEM	MITIGATING FACTORS	YES	NO
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 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 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, as a Custodian you may have appropriately mitigated the considerable risk factors and, therefore, notification is not required. In some circumstances, as a Custodian you may decide that a notification is necessary even when mitigating factors are present, especially when all of the foregoing considerable factors are involved. As a Custodian, you must consider that each situation is unique and all factors should be considered.

IV. What is the meaning of a "reasonable basis"?

A "reasonable basis" means that, based on their professional judgement, the Custodian can understand the incident and other relevant information – such as privacy, security or legal recommendations – and has the capacity to decide whether the considerable factors in assessing risk of harm apply to the situation at hand or not.

V. What information must be included when notifying an affected individual?

When notifying an affected individual, the notice must be in writing and must include the following elements:

1. Custodian information

- The name of the Custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure.
- 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.

2. Incident description

- A description of the circumstances of the loss or unauthorized access or disclosure.
- The date on which (or period of time within which) the loss or unauthorized access or disclosure occurred.

3. Type of information involved

- 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.)

4. Risk of harm

- A non-identifying description of the risk of harm to the individual as a result of the loss or unauthorized access or disclosure. The description must not identify an individual, but should include the following information:
  - The type of harm
  - An explanation of how the risk of harm was assessed
- 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.
- 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.
- 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.

5. Additional Information

- Any other information that the Custodian considers to be relevant to the affected individual.
- 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 regards to the loss or unauthorized access or disclosure.
- Contact information for the OIPC.

VI. What information must be included when giving notice to the Minister?

When notifying the Minister, the notice must include the following information submitted in writing on the form approved by the Minister (see section VIII for information on the form).

1. Custodian information

- The name of the Custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure.
- 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.

2. Incident description

- A description of the circumstances of the loss or unauthorized access or disclosure.

3. Type of information involved

- 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.)

4. Risk of harm

- 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:
  - The type of harm
  - An explanation of how the risk of harm was assessed
- 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.
- 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.

5. Additional information

- Any other information that the Custodian considers to be relevant.

VII. What information must be included when giving notice to the Commissioner?

The notice must include the following information submitted in writing on the form approved by the Commissioner (*see section XI for information on the form*).

1. Custodian information

- The name of the Custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure.
- 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.

2. Incident description

- A description of the circumstances of the loss or unauthorized access or disclosure.
- The date on which (or period within which) the loss or unauthorized access or disclosure occurred.
- The date the loss or unauthorized access or disclosure was discovered.

3. Type of information involved

- 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.)

4. Risk of harm

- 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:
  - The type of harm
  - An explanation of how the risk of harm was assessed
- 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.
- 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.

5. Additional information

- Any other information that the Custodian considers to be relevant.

VIII. Where can I find informative resources on how to report a breach, including a breach report form?

The Office of the Privacy Commissioner provides guidance on how to report a breach including a breach report form that you may use which can be found here.

IX. Where can I find the HIA Guidelines on the Duty to Notify?

The HIA Guidelines on the Duty to Notify can be found here.

X. Where can I find the form used to notify the Minister?

The Notification to Alberta's Minister of Health Form can be found here.

XI. Where can I find the form used to notify the Commissioner?

The notification to the Commissioner Form can be found here.

XII. Where can I find a sample notification letter to submit to an affected individual?

Please see Appendix 1 for a sample notification letter to submit to an affected individual.

APPENDIX 1

Notification Sample to an Affected Individual

Priority Care Clinic File # 14344 [***Custodian's file reference number***]

March 22, 2019 [***Date***]

Ms. Love Powers [***Name and address of affected individual***]
14 Heart Avenue SW
Calgary, AB T2T 2T2

Dear Ms. Powers, [***Title and name of affected individual***]

This notice is to advise you that your health information involving your diagnostic, treatment and care information [***State type of information involved***] under the custody and control of [***Name of Custodian***] was inappropriately accessed by a staff member while working on the patient records on Alberta Netcare [***State type of incident and describe circumstances of the loss, unauthorized access or disclosure***] on March 20, 2019 [***Date or time period of the incident***].

This notice is being provided to you in accordance with the requirement to notify an affected individual of an unauthorized access [***State type of incident: loss or unauthorized access or disclosure***] to their health information pursuant to Section 60.1 of the Health Information Act (HIA), and as a precautionary measure to prevent or reduce possible risk of harm to you.

The type of information accessed by one of the staff was the results of your laboratory tests. [***type of information involved***] We have conducted a risk of harm assessment and determined that because this type of information has the potential to cause harm, such as embarrassment, there is a potential for misuse. [***Risk of harm involved and assessed***]

We already conducted investigation of the staff and a disciplinary action will be implemented. Likewise, their access to Netcare has been revoked. Also, to prevent same issue to occur in the future, Priority Care Clinic is requiring all its staff to retake privacy training. [***Description of steps taken to reduce risk of harm to individual and future loss, unauthorized access or disclosure***]

If you have concerns regarding the confidentiality and security of your information in Netcare, we would recommend you obtain a copy of your Netcare Audit Log. [***Description of steps individual may be able to take to reduce risk of harm***] This log will show you the names of any individual who had accessed your Netcare record including the date the access occurred and the activities the individual undertook in your record. The Netcare Audit Log can be obtained by contacting the Alberta Health Freedom of Information and Protection of Privacy Office at 1.780.422.5111 or by emailing disclosure@ahs.ca.

Please be advised that the Office of the Information and Privacy Commissioner (OIPC) of Alberta has the authority to investigate any contraventions of the Health Information Act. If you would like to report any concerns to the Commissioner, please contact the OIPC Calgary Office at 1.403.297.2728 or email generalinfo@oipc.ab.ca. [***Statement that affected individual has the right to complain or request investigation to OIPC as well as OIPC contact information***]

If you have further questions concerning this incident, please feel free to reach me at 1.403.222.8282 or privacy@prioritycareclinic.com. [***Contact information relevant to the affected individual***]

Thank you,

[***Name and address of Custodian or Privacy officer or responsible affiliate that could answer queries of affected individual***]

Shania Smith-Coo
Privacy Officer
Priority Care Clinic
888 Harmony Bldg. 4th Street SW
Calgary, AB T8T 2T8