Chapter 14

Duty to Notify

Health Information Act Guidelines and Practices Manual

AUGUST 2018

Alberta

Alberta Health, Government of Alberta

August 2018

Health Information Act Guidelines and Practices Manual. Chapter 14: Duty to notify

This publication is a practical reference tool for the application of Alberta's *Health Information Act* (HIA or the *Act*).It is designed to assist all custodians that are subject to the *Act*.

The Guidelines and Practices Manual provides supplementary information regarding the HIA and Regulations. The Manual explains roles and responsibilities with respect to the administration of the *Act*.

The Manual is intended to provide guidelines and suggest best practices, not binding rules. The Manual also takes into consideration significant decisions of the Information and Privacy Commissioner.

All scenarios and examples provided are illustrative only and should not be viewed as authoritative statements of the law. This manual is not to be used as a substitute for legal advice. In case of any doubt as to the proper application of the *Act*, please consult with your privacy coordinator or legal counsel.

This edition of the Guidelines and Practices Manual incorporates amendments to the HIA up to August 31, 2018.

For further information about the use of the Guidelines and Practices Manual, please contact:

Alberta Health
HIA Help Desk
P.O. Box 1360, Station Main
Edmonton, Alberta T5J 2N3
Email: HIAHelpDesk@gov.ab.ca
Phone: 780-427-8089
Fax: 780-422-1960

This publication is available online only

Chapter Fourteen Duty to Notify

The *Health Information Act* and the regulations made under it establish the rules that must be followed for the collection, use, disclosure and protection of health information in the health sector. The *Health Information Act Guidelines and Practices Manual* is designed as a reference tool to help custodians and affiliates apply and administer the *Act.*

The *Manual* is intended to explain the legislation and to offer guidance on approaches, procedures and best practices. The information contained in the *Manual* is not meant to present binding rules. Any examples used are illustrative only and should not be used as authority for any decisions made under the *Act.*

The chapters of the *Manual* generally follow the scheme and order of the *Act.* A few chapters have been added to cover administrative processes and the first chapter is an overall introduction to the *Act*. At the back of many of the chapters are *'Things to Remember'.* These pages include bullet summaries of the important things to remember in the preceding chapter and, in some cases, decision flow charts or tables. They are meant to be used by readers as quick reminders or checklists about a particular topic but are not meant as a substitute for the more comprehensive chapter content or for referring to the *Act* and the regulations.

The *Act* and regulations can be found at: http://www.qp.alberta.ca/

There are a number of Appendices at the back of the *Manual.* These include forms, model letters, a detailed implementation checklist and components for agreements under the *Act.*

Best practices and examples used in the *Manual* should be considered as guidelines only. They are in boxes accompanying the text.

References to Practice Notes from the Office of the Information and Privacy Commissioner (OIPC) should also be considered as guidelines only since they are based upon practices related to the *Health Information Act (HIA),* the *Freedom of Information and Protection of Privacy (FOIP) Act* and the *Personal Information Protection Act (PIPA).*

Orders from the Office of the Information and Privacy Commissioner (OIPC) are binding on the parties to reviews and investigations related to the Health Information Act, the FOIP Act and PIPA.

Health Information Act, FOIP Act and PIPA Orders are distinguished by their numbering in the Commissioner's Office. HIA Orders are identified with the letter H (i.e., H2002-001), FOIP Orders are identified with the letter F (i.e., F2002-001) and PIPA Orders are identified with the letter P (i.e., P2006-001).

For information about the Office of the Information and Privacy Commissioner, see the Website for the OIPC at: http://www.oipc.ab.ca.

Portions of the *Manual* have been adapted from the *Freedom of Information and Protection of Privacy Guidelines and Practices (2000)* published by Service Alberta. We gratefully acknowledge this contribution.

For information about the *FOIP Act,* see the Website for the *Freedom of Information and Protection of Privacy Act* at: http://www.servicealberta.ca/foip/

For information about the *Personal Information Protection Act,* (PIPA) see the website for Private Sector Privacy at: http://pipa.alberta.ca

If there is any doubt as to the proper application of the *Act,* readers should request advice from the *Health Information Act* Coordinator (or the affiliate responsible for administering the *Act*) in their organization.

For further information about the administration or interpretation of the *Act,* please contact:

HIA Help Desk, Alberta Health
780-427-8089 (Tel), Toll free 310-0000-780-427-8089
780-422-1960 (FAX) or
Email: hiahelpdesk@gov.ab.ca.
The Website for Alberta Health is: http://www.health.alberta.ca

Throughout the *Manual* there are references to “Minister” and “Department”. These refer to the Minister responsible for the *Health Information Act,* currently the Minister of Health, and the Department of Alberta Health, respectively.

Chapter 14

Duty to Notify

14.1 Overview of Chapter Fourteen

This Chapter will cover:

- the duties of custodians and affiliates to notify;
- what a loss, unauthorized access or disclosure is;
- what to do if your organization experiences a loss, or unauthorized access or disclosure;
- how to assess whether there is a risk of harm to an individual;
- how to notify the Minister, Commissioner, and affected individual(s);
- how to prevent a future loss, unauthorized access or disclosure; and
- the offence provisions relevant to the duty to notify and failing to safeguard information.

14.2 Introduction to the Duty to Notify

In June 2014, the *Health Information Act* was amended to require a custodian to as soon as practicable give notice in accordance with the regulations of a loss of or any 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 an individual as a result of the loss or unauthorized access or disclosure.

Notice is to be given to the Information and Privacy Commissioner of Alberta, the Minister of Health, and the affected individual(s). The requirements for the form and content of these notices are set out in **section 8.2** of the *Health Information Regulation*.

The amendments also require an affiliate of a custodian who becomes aware of any loss 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.

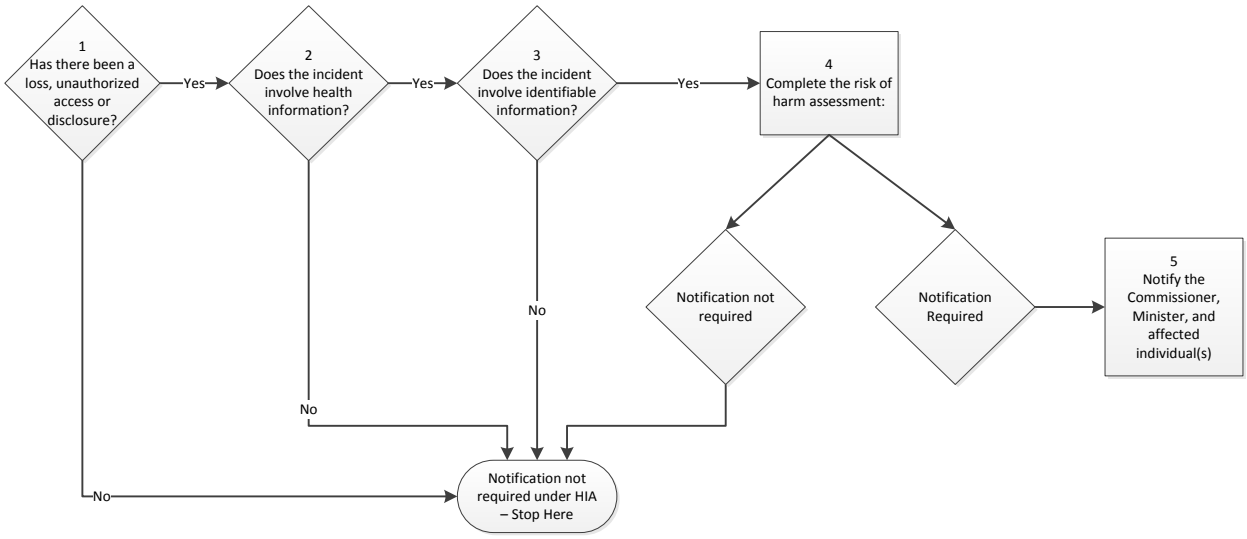
"**As soon as practicable**", in the context of **section 60.1 of the *Health Information Act***, means as soon as the affiliate or custodian becomes aware of the loss, unauthorized access or disclosure, and has the information that is necessary to properly execute the notice.

Custodians and affiliates are subject to offence penalties for failure to meet their duty to notify. Custodians are also subject to an offence provision for failure to take reasonable steps in

accordance with the regulation 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 and against any loss of health information.

Where notification is not required under the ***Health Information Act***, a custodian or affiliate may still be required to notify under contractual agreements or other privacy laws.

Assessment and Notification Process:



14.3 When is Notification Required?

Section 60.1 of the *Health Information Act* requires notification to the Commissioner, Minister and affected individual(s) where:

a) there has been **any loss of, or any unauthorized access to or disclosure of** individually identifying health information; and
b) 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.

Please note that the scenarios below are examples to illustrate where a loss, unauthorized access or disclosure has occurred. The scenarios do not include an assessment of risk of harm to determine if notification is required.

What is a Loss?

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. Note that this does not include where a custodian ceases to have custody or control of records due to a legitimate disclosure of the records to a successor custodian under **section 35(1)(q) of the *Health Information Act*.** A loss may involve physical or electronic records. Examples of loss may include where a medical record is lost by a storage facility contracted by a custodian, or where server data becomes corrupted, resulting in a loss of digital files.

Loss Scenario A – Theft of Files: A physician at a Calgary hospital took home a paper copy of medical files for 25 of her patients. The physician's home was broken into and the locked briefcase where the files were kept was stolen.

Loss Scenario B – Lost Laptop: In the course of an information technology project, a technician working for a custodian took home a laptop containing unencrypted individually identifying health information of about 200 patients. This laptop was accidentally left in a taxi and could not be retrieved.

Loss Scenario C – Loss of Files: A dental practice has an accidental fire in which all medical records are destroyed.

What is an Unauthorized Access?

An **unauthorized access** occurs where an individual accesses information that they were not authorized to access. Examples of unauthorized access may include where an electronic record is accessed in error by a health service provider, an individual deliberately accesses a record they are not authorized to access, or where an individual without the authority to access health information inappropriately accesses a filing cabinet containing individually identifying health information.

Unauthorized Access Scenario A – Access for Personal Use: A nurse working in an Edmonton hospital has an acquaintance in the hospital who has just given birth. For curiosity's sake, the nurse accesses the record of his acquaintance.

Unauthorized Access Scenario B – Hacking: An individual hacked into a hospital's computer network and the hospital's IT staff have determined that he accessed diagnostic, treatment and care information of multiple patients in the hospital.

Unauthorized Access Scenario C – Access in Error: In the course of providing treatment to a patient, a physician attempts to access the patient's electronic health record to obtain the patient's lab results. In error, the physician accesses the information of a different person with a similar name, who has never been the physician's patient.

What is an Unauthorized Disclosure

An **unauthorized disclosure** occurs where there has been a deliberate or accidental disclosure of individually identifying health information in contravention of the *Health Information Act*. Examples of unauthorized disclosure include where a fax is received by an individual who is not the intended recipient, or where a disclosure that can only be authorized with valid consent is made outside the terms of that consent.

Unauthorized Disclosure Scenario A – Incorrectly Addressed Letter: A letter regarding an Albertan's cancer screening was sent to the Albertan's former address and the letter was opened by another person who now resides at that address.

Unauthorized Disclosure Scenario B – Improper Disposal: A contractor assigned by a clinic to shred patients' medical records instead dumped the records in a landfill, where they were found by a waste disposal employee.

Unauthorized Disclosure Scenario D – Incomplete Destruction of Information: A medical clinic's shredding machine broke mid-way through the shredding of papers containing individual identifying health information. The medical office throws the partially shredded documents in the dumpster, where they are seen by a waste disposal employee.

Unauthorized Disclosure Scenario C – Disclosure Outside of Consent: An individual's employer required proof of the employee's hospital stay in order to accept the claim of time off. The individual provided consent for the hospital to disclose the duration of her stay to her employer. Instead of just providing the duration of stay, the hospital disclosed the individual's discharge summary, which included diagnostic, treatment and care information, to the employer.

Disclosure of Non-Identifying Information

If the identity of the individual who is the subject of the information cannot be readily ascertained from the information, then the information is considered non-identifying. The *Health Information Act* authorizes the collection, use and disclosure of non-identifying information for any purpose. As such, any use or disclosure of non-identifying information is authorized under the *Health Information Act*. For more information, see **sections 5.2.1, 7.2.1, 7.3, 8.2, 8.2.1 of the HIA Guidelines and Practices Manual**.

14.4 Affiliates Duty to Notify

Section 60.1(1) of the *Health Information Act* 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.

Form and Manner of the Notification

The custodian must establish policies and procedures to direct their affiliates as to how this duty is to be carried out. For example, the custodian may wish to be notified through a telephone call, an email, a submitted form, or another method.

If the custodian has established requirements regarding the form and content of this notice, **section 8.2(1)(a) of the *Health Information Regulation*** requires the affiliate to execute the notice in accordance with the custodian's requirements.

If the custodian has not established requirements regarding the form and content of this notice, **section 8.2(1)(b) of the *Health Information Regulation*** requires the notice to be in writing and include:

1. A description of the circumstances of the loss or unauthorized access or disclosure;
2. The date on which or period of time within which the loss or unauthorized access or disclosure occurred;
3. The date on which the loss or unauthorized access or disclosure was discovered; and
4. A description of the information that was lost or that was the subject of the unauthorized access or disclosure.

Accountability

Regardless of the chosen notification method, as a best practice, the custodian and affiliate should have in place a record of this notification so compliance with the Act can be proven.

14.5 Custodian's Duty to Notify

Subsections 60.1(2) and (3) of the *Health Information Act* require a custodian to notify the Commissioner, Minister 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.

Assess Risk of Harm

Where a custodian becomes aware of any loss of, unauthorized access to, or disclosure of individually identifying health information in their custody or control (whether they discovered it themselves or were notified of it by an affiliate under **section 60.1(1) of the *Health Information Act***), they must 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.

Notification

Where the custodian determines a risk of harm exists, they must, as soon as practicable, give notice in accordance with the regulations.

If the custodian is not sure if any loss of, unauthorized access to, or disclosure of individually identifying health information in their custody or control has occurred, a custodian should continue to investigate the situation to determine if a loss or unauthorized access or disclosure has

occurred. If the custodian cannot be certain that a loss or unauthorized access or disclosure has occurred, they are not required to notify, but may consider notifying if they deem it necessary.

14.6 Assessing 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.

14.6.1 Factors to Consider

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

i. whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;
ii. whether there is a reasonable basis to believe that the information has been misused or will be misused;
iii. whether there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud;
iv. 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;
v. 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;
vi. in the case of electronic information, whether the custodian is able to 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;
vii. in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was
    i. destroyed, or
    ii. rendered inaccessible or unintelligible;

viii. 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;

ix. 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.

If a custodian is able to demonstrate that a circumstance set out in section 8.1(1)(f) to (i) applies in the case of the loss or unauthorized access or disclosure, the custodian is not required to give notice under section 60.1(2) of the Act.

The **Risk of Harm Checklist** in **Appendix 3** can be used to assist custodians in ensuring that they have considered all required factors under **section 8.1(1) of the *Health Information Regulation***.

Reasonable Basis

A **reasonable basis** exists where a custodian can, based on their professional judgement, understanding of the incident or other relevant information such as recommendations from privacy, security, and legal teams, commit to a decision that the factor is applicable in the situation.

The Factors in Detail

Part A: Circumstances where notification is required:

8.1(1)(a) Whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;

- This factor addresses whether there is a reasonable basis to believe that the information actually has been accessed or will likely be accessed based on the level of security protecting the information. This does not include where information has been transmitted in

an insecure fashion (e.g. non-encrypted email) but there is no likelihood that the information will be accessed by an unintended recipient.

- For example, where the custodian can identify from an audit of the access logs of their electronic medical record that an affiliate has accessed information they were not authorized to access.
- If due to a technical error, a custodian unintentionally makes an individual's health information publicly available on their website, the custodian would need to consider that the health information has been disclosed to a person.
- Some factors that a custodian should consider when making this assessment include:
- In the case of a loss or disclosure of information, was the information in a form that would be accessible to anyone who discovered or received the information?
    - Can the custodian remotely destroy the information to prevent it from being accessed?

8.1(1)(b) Whether there is a reasonable basis to believe that the information has been misused or will be misused;

- This factor addresses a person's intent or information about how the information has been or may be used. For example, where the loss, unauthorized access or disclosure was intentional, this factor applies. Where the incident was not intentional, but was inadvertently disclosed to a person who may have malicious intent, this factor applies. In situations where the intent is unknown, if there is evidence of misuse or potential misuse this factor applies. Even if there is no malicious intent, this factor will still apply if there is a reasonable basis to believe that the information has or will be misused.
- For example, where the custodian is aware that the individual who accessed or received the information intends to use it to embarrass the individual who is the subject of the information. Even if the individual who accessed or received the information does not intend to use it to embarrass the individual but might nonetheless inadvertently do so, this factor would still apply.
- Some factors that a custodian should consider when making this assessment include:
    - Does the individual who accessed or received the information have a personal relationship with the individual who is the subject of the information?
    - Does the individual who accessed or received the information have a malicious intent?
    - How did the individual who accessed the information use the information?
    - In the case of a loss or disclosure of information, was the information in a form that would be accessible to anyone who discovered or received the information?

8.1(1)(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;

- This factor addresses the type of information involved in the incident and its ability to be used for fraudulent purposes or to commit identity theft.
- For example, where the custodian is aware that the information that has been lost contains registration information such as contact information, personal health numbers or credit card information.
- Some factors that a custodian should consider when making this assessment include:
    - Is the information of a type that could be used for identity theft or fraud?

8.1(1)(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;

- This factor addresses the nature and sensitivity of the information in relation to the individual.
- For example, information that includes specific information about an individual's physical or mental health, such as lab results or diagnoses, or information that could be used to track the individual or their financial information, such as contact information or credit card information.
- For example, the lost record is from a health facility within a correctional facility, thus identifying the individual as an inmate.
- Note that a custodian should consider the individual who is the subject of the information as well as the type of information involved when making this assessment.
    - For example, consider the individual's current and past emotional and mental health. Also, the type of information involved is important. For example, if the information involved is an appointment reminder the chance of harm or damage may be less compared to if the information involved is an individual's test results. Consider whether the individual would be concerned with the release of this information.

8.1(1)(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;

This factor addresses the impact of the breach on the provision of health services.

- For example, where an emergency room patient's diagnosis depends on the results of a lab test and the lab results are faxed to the wrong fax number. This could result in the delay of the diagnosis, thereby having an adverse impact on treatment.

- Some factors that a custodian should consider when making this assessment include:
    - Has the loss, access, or disclosure resulted in a delay or prevented a health service from being provided to the individual?
    - Is the information necessary for an urgently needed health service to the individual who is the subject of the information?
    - Was the loss, access, or disclosure discovered in a reasonable amount of time to allow for any adverse impact on the provision of a health service to be mitigated?

In addition to considering the factors in **sections 8.1(1)(a)-(e)**, if there are any other factors that are relevant which may indicate risk of harm to the individual, those factors should also be considered.

- Some factors that a custodian should consider when making this assessment include:
    - Is the custodian aware of any circumstances, not included in these factors, which would indicate a risk of harm to the individual who is the subject of the information?
    - How many individuals were affected by the loss, unauthorized access or disclosure?
    - Whether there is reasonable basis to believe that the individual whose information was lost, accessed, or disclosed without authorization is especially sensitive to any possible breaches of their privacy (for example, if their Netcare account is masked and suffered an unauthorized access).

Part B: Circumstances where notification is not required:

Where any of the above factors apply to a loss, unauthorized access or disclosure of individually health information, the risk of harm may be sufficiently mitigated by the circumstances found below. If the factors below apply, the custodian is not required to give notice under section **60.1(2) of the *Health Information Act***:

8.1(1)(f) In the case of electronic information, whether the custodian is able to 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.

- For example, notification would likely not be required:

- where an email containing individually identifying health information is sent to the wrong email address, but the email was properly encrypted and therefore cannot be accessed by the recipient; or
- where a laptop or other device is lost, but is properly encrypted and password protected, and therefore cannot be accessed by an individual who finds the laptop or device.

- Some factors that a custodian should consider when making this assessment include:
  - Was the information secured in accordance with industry standards?
  - Has the loss, unauthorized access or disclosure put the information in the hands of an individual or group that could have the capability to bypass the information security?
  - In the case of a loss or disclosure of information, was the information in a form that would be accessible to anyone who discovered or received the information?

8.1(1)(g) In the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was

i. destroyed, or
ii. rendered inaccessible or unintelligible;

- For example, notification would likely not be required:
  - where information was lost in a fire or flood; or
  - where medical slides are broken as they fall out of a truck.
- Some factors that a custodian should consider when making this assessment include:
  - As a result of the loss, was the information completely destroyed?

8.1(1)(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;

- For example, where a locked briefcase is left in a public place, but is then recovered and it is clear that the briefcase has not been opened.
- Some factors that a custodian should consider when making this assessment include:
  - Was the information retrieved?
  - Is there evidence that the information was accessed?
  - Was the information in a form that was easily accessible?

8.1(1)(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,

- **Section 63 of the *Health Information Act*** requires custodians to implement policies that facilitate the implementation of the Act within their organization. **Section 60 of the *Health Information Act*** requires custodians to implement reasonable safeguards to protect the confidentiality and integrity of health information and the privacy of the individuals who are the subjects of that information. As such, a custodian must have in place a policy or policies that address the requirements of **section 60 of the *Health Information Act*.** These policies would prohibit the receiving custodian from further disclosing the information in contravention of the *Health Information Act*.
- Some factors that a custodian should consider when making this assessment include:
  - Is the individual who received the information or accessed the information a custodian or affiliate?
  - Does the custodian or affiliate have policies and procedures in place regarding the adequate protection of health information?
  - Is the custodian or affiliate bound by a confidentiality oath?

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

- Some factors that a custodian should consider when making this assessment include:
  - Was the custodian or affiliate accessing the information in an attempt to provide a health service to the individual who is the subject of the information or to another individual?
  - Was the custodian or affiliate authorized to have access to the information or the system containing the information?
  - Did the custodian or affiliate use another individual's access credentials to gain access to the information?
  - Did the custodian or affiliate access the information deliberately for an unauthorized purpose?
  - Did the custodian or affiliate who accessed the record do so for personal reasons?

- Did the custodian or affiliate who received the disclosure have a personal relationship with the individual who was the subject of the information?

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.

- Note that this is a two-part factor: a custodian or affiliate is permitted under **section 27(1)(g) of the *Health Information Act*** to collect, use or disclose individually identifying health information for internal management purposes. As such, where a custodian or affiliate views health information that has been disclosed to them, realizes that it was disclosed to them in error and uses that information (such as health services provider contact information) to report the breach to the custodian or affiliate who disclosed the information, they meet both parts of **section 8.1(1)(i)(iv)**.
- Some factors that a custodian should consider when making this assessment include:
  - Did the custodian or affiliate who received the fax (an unauthorized disclosure) use the information beyond determining that the fax was not intended for them?
  - Did the custodian or affiliate who received the fax disclose the information to another person who was not the sender of the fax?
  - Did the custodian or affiliate who received or accessed the record use or disclose the information for another purpose other than determining that the record was accessed or disclosed in error or in mitigating the access?

In addition to considering the factors in sections **8.1(1)(f)-(i),** if the custodian is aware of any other factor that is relevant to the potential mitigation of the risk, that factor should also be considered.

- For example, where the custodian can confirm that the individual who received the unauthorized disclosure has destroyed the information and did not retain any copies.
- Some factors that a custodian should consider when making this assessment include:
  - Is the custodian aware of any reason, not included in these factors, which would indicate that the risk has been appropriately mitigated?
  - Can the custodian confirm that the information was properly destroyed by the individual who received or found the information?
  - Can the custodian confirm that the loss, unauthorized access or disclosure was unintentional?

Where a custodian is able to demonstrate that factors from Part B are present, the factors from Part A may be appropriately mitigated and therefore notification is not required. In some

circumstances, the custodian may decide that notification is necessary even when factors from Part B are present.

Things to Consider

Where the loss, unauthorized access to, or disclosure of individually identifying health information in the custody or control of a custodian has or will impact upon the provision of health services, or is deliberate, notification should be strongly considered. In addition, where the individual who accesses or receives the information is not a custodian or affiliate under the *Health Information Act*, notification should be strongly considered.

14.6.2 Examples of Risk Assessment

The following fictional scenarios present examples of applying the factors set out in **section 8.1(1) of the *Health Information Regulation*** that a custodian must consider when assessing risk of harm. In each scenario, a loss, unauthorized access or disclosure of individually identifying health information has occurred and the custodian must now apply the factors to assess whether there is a risk of harm to the individual who is the subject of the information as a result of the incident. Each of the factors from Part A and Part B will be assessed against the circumstances of each scenario. As per the above section, where a custodian is able to demonstrate that factors from Part B are present, the factors from Part A may be appropriately mitigated and therefore notification is not required, but may still be given at the custodian's discretion.

Risk of Harm Analysis Example 1 – Unauthorized Access:

Dr. Smith, in preparation for a patient's visit, attempts to access the patient's record on Alberta Netcare to view the results of recent lab tests. After opening the record, Dr. Smith realizes that he has opened the record of an individual with a similar name, but who is not his patient. Dr. Smith immediately closed the file.

Part A: Circumstances where Notification is required		
Factor	**Applicable/Not Applicable**	**Rationale**
8.1(1)(a) whether there is a reasonable basis to believe that the	Applicable	Dr. Smith accessed a file for an individual who was not his patient.

information has been or may be accessed by or disclosed to a person;		
8.1(1)(b) whether there is a reasonable basis to believe that the information has been misused or will be misused;	Not Applicable	In this scenario, there is no reasonable basis to believe that Dr. Smith misused or will misuse the information. Dr. Smith has no personal connection to the individual whose information he viewed.
8.1(1)(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;	Applicable	An individual's Alberta Netcare record contains registration information and diagnostic, treatment and care information, both of which could be used for identity theft or to commit fraud.
8.1(1)(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;	Applicable	Alberta Netcare contains diagnostic, treatment and care information and registration information, which could cause embarrassment or physical, mental, or financial harm to, or damage the reputation of the individual
8.1(1)(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	Not Applicable	The unauthorized access did not, and will not adversely affect the provision of a health service to the individual.

who is the subject of the information;		
There are other relevant factors	Not Applicable	The custodian is not aware of any other relevant factor that could indicate a risk of harm to the individual who is the subject of the information.
Part B: Circumstances where notification is not required		
Factor	**Applicable/ Not Applicable**	**Rationale**
8.1(1)(f) in the case of electronic information, whether the custodian is able to 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;	Not Applicable	The information was accessed.
8.1(1)(g) in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in	Not Applicable	This factor is not relevant as the incident does not involve the loss of information.

circumstances in which the information was (i) destroyed, or (ii) rendered inaccessible or unintelligible;		
8.1(1)(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;	Not Applicable	In this case, this factor is not relevant as the incident does not involve the loss of information.
8.1(1)(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	Applicable	Dr. Smith, the individual who accessed the information: (i) is a custodian who is bound by the *Health Information Act*; (ii) is subject to confidentiality policies and procedures; (iii) accessed the information in a manner consistent with his role as a health services provider and did not do it for an improper purpose; and (iv) did not use or disclose the information beyond determining that he accessed it in error.

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.		
There are other relevant factors	Applicable	The custodian is aware that the unauthorized access was an error and was not a deliberate attempt to breach the privacy of the individual who was the subject of the information.

As Dr. Smith accessed information that he did not have authority to access, this is an example of unauthorized access.

Part A Assessment:

- 8.1(1)(a). There is a reasonable basis to believe that any person has accessed or will be able to access the health information.
- 8.1(1)(c). There is a reasonable basis to believe that the health information could be used for identity theft or committing fraud.
- 8.1(1)(d). 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.

As one or more factors in Part A were applicable notification may be required.

Part B Assessment:

- 8.1(1)(i). The custodian can demonstrate that the information has been accessed and that the only person who accessed the information or to whom the information was disclosed:

- is a custodian or affiliate;
- is subject to confidentiality policies and procedures that meet the requirements of section 60 of the Act;
- accessed the health information in a manner consistent with the person's duties as a custodian or affiliate and not for an improper purpose; and
- did not use or disclose the information beyond determining that the access or disclosure was in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure.

- The custodian has considered other relevant factors.

As one or more of the factors in Part B is applicable, the risk is appropriately mitigated and notification is not required.

NOTIFICATION IS NOT REQUIRED.

Risk of Harm Assessment Example 2 – Unauthorized Disclosure:

A family physician attempted to fax a referral form to Dr. Graham, but accidentally used a different fax number belonging to Dr. Smith. Dr. Smith is also a custodian under the *Health Information Act*, working in a different clinic. The family physician immediately noticed the error and asked Dr. Smith to shred the referral form. Dr. Smith shredded the referral form and the family physician correctly faxed the form to Dr. Graham.

Note: In this case, Dr. Smith is the individual who received the disclosure. The family physician is the individual who caused the unauthorized disclosure and is the custodian responsible for assessing the risk of harm in this incident.

Part A: Circumstances where notification is required		
Factor	**Applicable/Not Applicable**	**Rationale**
8.1(1)(a) whether there is a reasonable basis to believe that the	Applicable	Dr. Smith accessed a file for an individual who was not his patient.

information has been or may be accessed by or disclosed to a person;		
8.1(1)(b) whether there is a reasonable basis to believe that the information has been misused or will be misused;	Not Applicable	As Dr. Smith is a custodian under the HIA who notified the family physician and immediately shredded the information, there is no reasonable basis to believe that the information has been or will be misused.
8.1(1)(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;	Applicable	The information contained in the referral form included registration information and diagnostic, treatment and care information, both of which could be used for identity theft or fraud.
8.1(1)(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;	Applicable	The referral form contains individually identifying diagnostic, treatment and care information which is sensitive and could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual.
8.1(1)(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	Not Applicable	The unauthorized access did not, and will not adversely affect the provision of a health service to the individual. As the family physician immediately noticed the error, he was able to resend the form to Dr. Graham without causing delay in the provision of health services to the individual.

who is the subject of the information;		
There are other relevant factors	Not Applicable	The custodian is not aware of any other relevant factor that could indicate a risk of harm to the individual who is the subject of the information.

Part B: Circumstances where notification is not required		
Factor	**Applicable/ Not Applicable**	**Rationale**
8.1(1)(f) in the case of electronic information, whether the custodian is able to 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;	Not Applicable	It cannot be demonstrated that the information was secured in a manner or form that would render the information inaccessible or unintelligible to a person not authorized to receive it. The information was sent via fax and was viewable to anyone who had access to the receiving fax machine. As it was not encrypted or password-protected, the information was read by Dr. Smith, who was not the intended recipient.
8.1(1)(g)	Not Applicable	This factor is not relevant as it the incident does not involve the loss of information.

in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was (i) destroyed, or (ii) rendered inaccessible or unintelligible;		
8.1(1)(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;	Not Applicable	In this case, this factor is not relevant as the incident does not involve the loss of information.
8.1(1)(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	Applicable	Dr. Smith, the individual who accessed the information: (i) is a custodian who is bound by the *Health Information Act*; (ii) is subject to confidentiality policies and procedures; (iii) accessed the information in a manner consistent with his role as a health services provider and did not do it for an improper purpose; and (iv) did not use or disclose the information beyond determining that he accessed it in error.

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.		
There are other relevant factors	Applicable	The information was destroyed upon request.

Dr. Smith was not the intended recipient of the disclosure; therefore, this is an example of unauthorized disclosure.

Part A Assessment:

- 8.1(1)(a). There is a reasonable basis to believe that a person has accessed or will be able to access the health information.
- 8.1(1)(c). There is a reasonable basis to believe that the health information could be used for identity theft or committing fraud.
- 8.1(1)(d). 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.

As one or more factors in Part A are applicable, notification may be required.

Part B Assessment:

- 8.1(1)(i). The custodian can demonstrate that the information has been accessed and that the only person who accessed the information or to whom the information was disclosed:
  - is a custodian or affiliate;
  - is subject to confidentiality policies and procedures that meet the requirements of section 60 of the Act;
  - accessed the health information in a manner consistent with the person's duties as a custodian or affiliate and not for an improper purpose; and
  - did not use or disclose the information beyond determining that the access or disclosure was in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure.
- The custodian has considered other relevant factors.

As one or more of the factors in Part B is applicable, the risk is appropriately mitigated and notification is not required.

NOTIFICATION IS NOT REQUIRED

Risk of Harm Assessment Example 3 – Loss:

While providing IT services for a medical clinic, a computer technician misplaced a USB storage device containing individually identifying health information of about 30 patients who visited the medical clinic within the last week. The device could not be recovered. The information on the device had been backed up and a copy of it remains in the clinic's computer system. The device was properly encrypted and password-protected.

In this case, the computer technician (an affiliate of the custodian(s) at the medical clinic) is the individual who caused the loss. The custodian who had custody or control of the information before it was lost is the custodian responsible for assessing the risk of harm in this incident.

Part A: Circumstances where Notification is required		
Factor	**Applicable/Not Applicable**	**Rationale**
8.1(1)(a) whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;	Not Applicable	There is no reasonable basis to believe that any unauthorized person will be able to access the lost health information contained on the device as it was properly encrypted and password-protected.
8.1(1)(b) whether there is a reasonable basis to believe that the information has been misused or will be misused;	Not Applicable	Given that the device had adequate security safeguards, there is no reasonable basis to believe that the information has been or will be misused.
8.1(1)(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;	Not Applicable	Given that the device had adequate security safeguards, there is no reasonable basis to believe that an unauthorized person will be able to access the information and use it for the purpose of identity theft or to commit fraud.

8.1(1)(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;	Applicable	The USB contains diagnostic, treatment and care information, and registration information, which could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individuals who are the subject of the information.
8.1(1)(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;	Not Applicable	There is no reasonable basis to believe that the loss has or will adversely affect the provision of a health service to any of the affected individuals.
There are other relevant factors	Not Applicable	The custodian is not aware of any other relevant factor that could indicate a risk of harm to the individuals who are the subject of the information.
Part B: Circumstances where notification is not required		
Factor	**Applicable/ Not Applicable**	**Rationale**
8.1(1)(f) in the case of electronic information, whether the custodian is able to demonstrate that the information was	Applicable	The device was properly encrypted and password protected, thereby preventing the information from being accessed by an unauthorized person.

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;		
8.1(1)(g) in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was (i) destroyed, or (ii) rendered inaccessible or unintelligible;	Applicable	As the device was properly encrypted and password-protected, it can be demonstrated that the information in the lost USB device was secured and lost in a manner that would render the information inaccessible by an unauthorized person.
8.1(1)(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;	Not Applicable	In this case, this factor is not relevant as the information has not been recovered.

8.1(1)(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.	Applicable	In this case, this factor is not relevant as the information has not been accessed or disclosed.
There are other relevant factors	Applicable	The custodian is aware that the loss was not intentional. The information is suspected to have been misplaced, as opposed to having been stolen. It is unlikely that any individual who finds

		the USB will be aware of the content and will attempt to access the information contained therein.

Information that 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. Therefore, this incident is an example of loss.

Part A Assessment:

- 8.1(1)(d). 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.

As one or more factors in Part A are applicable, notification may be required.

Part B Assessment:

- 8.1(1)(f). The custodian can demonstrate that the information was encrypted and password protected, thereby rendering it inaccessible to an unauthorized person.
- 8.1(1)(g). The custodian can demonstrate that the health information involved was lost in a manner that renders the information inaccessible.
- The custodian has considered other relevant factors.

As one or more of the factors in Part B is applicable, the risk is appropriately mitigated and notification is not required.

NOTIFICATION IS NOT REQUIRED

Risk of Harm Assessment Example 4 – Unauthorized Access:

Dr. Brown is an affiliate working within a facility of a regional health authority. Dr. Brown recently went through a bad divorce and accessed the health information of his ex-wife on Alberta Netcare. The ex-wife is not in a care relationship with Dr. Brown. Dr. Brown's ex-wife requested a copy of her Netcare Audit Log, discovered the access, and reported this access to the regional health authority.

In this case, Dr. Brown is an affiliate. The regional health authority is the custodian responsible for assessing the risk of harm in this incident.

Part A: Circumstances where notification is required		
Factor	**Applicable/Not Applicable**	**Rationale**
8.1(1)(a) whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;	Applicable	Due to the audit log, there is a reasonable basis to believe that an unauthorized person has accessed the information.
8.1(1)(b) whether there is a reasonable basis to believe that the information has been misused or will be misused;	Applicable	The information has been misused by Dr. Brown. There is also a reasonable basis to believe that the information will be subject to further misuse due to the nature of the relationship between Dr. Brown and his ex-wife.
8.1(1)(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;	Applicable	The Netcare record contains registration information and as such could be used for identity theft or fraud. Additionally, there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud given

		the fact that the unauthorized access was done deliberately.
8.1(1)(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;	Applicable	Netcare contains registration, diagnostic, treatment and care information which could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual.
8.1(1)(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;	Not Applicable	The unauthorized access did not, and will not adversely affect the provision of a health service to the individual.
There are other relevant factors	Applicable	The custodian is aware that the unauthorized access was a deliberate attempt to breach the privacy of the individual who was the subject of the information and that Dr. Brown has a personal relationship with the individual.

Part B: Circumstances where notification is not required		
Factor	**Applicable/ Not Applicable**	**Rationale**
8.1(1)(f) in the case of electronic information, whether the custodian is able to 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;	Not Applicable	The information has been accessed, and was not in a form that would cause this factor to apply.
8.1(1)(g) in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was (i) destroyed, or (ii) rendered inaccessible or unintelligible;	Not Applicable	This factor is not relevant as this incident does not involve a loss of information.

8.1(1)(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;	Not Applicable	In this case, this factor is not relevant as this incident does not involve a loss of information.
8.1(1)(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	Not Applicable	Dr. Brown, the individual who accessed the information: (i) is an affiliate who is bound by the *Health Information Act*; (ii) is subject to confidentiality policies and procedures; (iii) **did not** access the health information in a manner consistent with his duties, as he is not in a care relationship with his ex-wife. He accessed the information for an improper purpose; and (iv) used the information beyond determining that the access was in error and taking any steps reasonably necessary to address the unauthorized access or disclosure.

by or disclosed to the person in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure.		
There are other relevant factors	Not Applicable	The custodian is not aware of any other factor that would assist in mitigating risk.

As Dr. Brown did not have authority to access this individual's Netcare record, this is an example of unauthorized access.

Part A Assessment:

- 8.1(1)(a). There is a reasonable basis to believe that any person has accessed or will be able to access the health information.
- 8.1(1)(b) & 8.1(1)(c). There is a reasonable basis to believe that the health information will be misused or has been misused and that the health information could be used for identity theft or committing fraud.
- 8.1(1)(d). 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.
- The custodian has considered other relevant factors.

As one or more factors in Part A are applicable, notification may be required.

Part B Assessment:

As none of the factors in Part B are applicable, the risk is not mitigated and notification is required.

NOTIFICATION IS REQUIRED

Risk of Harm Assessment Example 5 – Unauthorized Disclosure:

A hospital clerk attempted to fax a referral form to a specialist, but accidentally used the wrong fax number. The information was accidentally sent to the personal fax machine of a member of the public, Ibadan Smith. Upon receipt of the form, Ibadan read the information in the referral form and contacted the hospital to let them know what she had received. The hospital resent the form to the correct number. The hospital also requested that Ibadan destroy or return the form to the hospital but Ibadan refused to do either.

In this case, Ibadan Smith is the individual who received the unauthorized disclosure. The hospital clerk (an affiliate of the regional health authority) is the individual who caused the unauthorized disclosure. The regional health authority is the custodian responsible for assessing the risk of harm in this incident.

Part A: Circumstances where notification is required		
Factor	**Applicable/Not Applicable**	**Rationale**
8.1(1)(a) whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;	Applicable	Ibadan has stated that she has received the information; therefore, the custodian has a reasonable basis to believe that the information has been accessed.
8.1(1)(b) whether there is a reasonable basis to believe that the information has been misused or will be misused;	Applicable	As Ibadan refuses to return or destroy the information, therefore there is a reasonable basis to believe that the information will be misused.
8.1(1)(c) whether there is a reasonable basis to believe that the information could be used for	Applicable	The information involved includes diagnostic, treatment and care information as well as registration information, both of which have the

the purpose of identity theft or to commit fraud;		potential to be used for identity theft or fraud.
8.1(1)(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;	Applicable	The referral form contains individually identifying diagnostic, treatment and care information which could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual.
8.1(1)(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;	Not Applicable	The unauthorized access did not, and will not adversely affect the provision of a health service to the individual.
There are other relevant factors	Applicable	The custodian is aware that the recipient of the information refuses to destroy or return the information. The custodian cannot determine whether or not the recipient will use or disclose the information further.
Part B: Circumstances where notification is not required		
Factor	**Applicable/ Not Applicable**	**Rationale**
8.1(1)(f)	Not Applicable	It cannot be demonstrated that the information was secured in a manner that would render the information

in the case of electronic information, whether the custodian is able to 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;		inaccessible or unintelligible by a person not authorized to access the information. The information was sent via fax and was viewable to anyone who had access to the receiving fax machine. As it was not encrypted or password-protected, the information was read by Ibadan, who was not the intended recipient.
8.1(1)(g) in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was (i) destroyed, or (ii) rendered inaccessible or unintelligible;	Not Applicable	This factor is not relevant as this incident does not involve a loss of information.
8.1(1)(h) in the case of a loss of information that is subsequently recovered by the custodian, whether the custodian can demonstrate that the information	Not Applicable	In this case, this factor is not relevant as this incident does not involve a loss of information.

was not accessed before it was recovered;		
8.1(1)(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.	Not Applicable	Ibadan Smith, the individual who accessed the information: (i) is **not** a custodian or affiliate who is bound by the *Health Information Act*; (ii) is **not** subject to confidentiality policies and procedures; (iii) did not access the information in a manner consistent with her duties as a custodian or affiliate, as she is not a custodian or affiliate. She may not have accessed the information for an improper purpose, however, the custodian cannot make this decision and therefore must err on the side of caution; and (iv) may use or disclose the information further as she refuses to destroy or return the information.

There are other relevant factors	Not Applicable	The custodian is not aware of any other factor that would mitigate a risk of harm.

Ibadan Smith was not the intended recipient of the disclosure; therefore, this is an example of unauthorized disclosure.

Part A Assessment:

- 8.1(1)(a). The custodian reasonably believes that any person has accessed or will be able to access the health information.
- 8.1(1)(b) & 8.1(1)(c). The custodian reasonably believes that the health information will be misused or has been misused and that he health information could be used for identity theft or committing fraud.
- 8.1(1)(d). The custodian reasonably believes 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.
- The custodian has considered other relevant factors.

As one or more factors in Part A are applicable, notification may be required.

Part B Assessment:

As none of the factors from Part B are applicable, notification is required.

NOTIFICATION IS REQUIRED

Risk of Harm Assessment Example 6 – Unauthorized Disclosure:

While attempting to fax lab results to a specialist, a family physician accidentally faxed the information to a dentist, Dr. Jones, instead. Recognizing that the fax was sent to her in error, Dr. Jones shredded the results, but did not notify the referring family physician. The referring family physician did not become aware of the incident until the intended recipient phoned the referring family physician three days later. As the intended recipient did not receive the results in time, urgently needed treatment for the patient was delayed. The family physician eventually discovered where the fax was misdirected and ensured that it had been destroyed.

In this case, the family physician is the individual who caused the unauthorized disclosure and is the custodian responsible for assessing the risk of harm. Dr. Jones is the individual who received the unauthorized disclosure.

Part A: Circumstances where Notification is required		
Factor	**Applicable/Not Applicable**	**Rationale**
8.1(1)(a) whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;	Applicable	As Dr. Jones received and reviewed information for an individual who was not her patient, the information was accessed.
8.1(1)(b) whether there is a reasonable basis to believe that the information has been misused or will be misused;	Not Applicable	Dr. Jones does not have a personal relationship with the patient. There is no reasonable basis to believe that the information has been or will be misused.
8.1(1)(c) whether there is a reasonable basis to believe that the information could be used for	Applicable	The information involved includes diagnostic, treatment and care information as well as registration information, both of which have the

the purpose of identity theft or to commit fraud;		potential to be used for identity theft or fraud.
8.1(1)(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;	Applicable	The lab test results could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual who is the subject of the information.
8.1(1)(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;	Applicable	The unauthorized disclosure did impact upon the provision of health services.
There are other relevant factors	Not Applicable	The custodian is not aware of any other relevant factor that could indicate a risk of harm to the individual who is the subject of the information.
Part B: Circumstances where notification is not required		
Factor	**Applicable/ Not Applicable**	**Rationale**
8.1(1)(f) in the case of electronic information, whether the custodian is able to demonstrate	Not Applicable	It cannot be demonstrated that the information was secured in a manner that would render the information inaccessible or unintelligible. The

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;		information was sent via fax and was viewable to anyone who had access to the receiving fax machine. As it was not encrypted or password-protected, the information was read by Dr. Jones, who was not the intended recipient.
8.1(1)(g) in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was (i) destroyed, or (ii) rendered inaccessible or unintelligible;	Not Applicable	This factor is not relevant as this incident does not involve a loss of information.
8.1(1)(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;	Not Applicable	In this case, this factor is not relevant as this incident does not involve a loss of information.

8.1(1)(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.	Applicable	Dr. Jones, the individual who accessed the information: (i) is a custodian who is bound by the *Health Information Act;* (ii) is subject to confidentiality policies and procedures; (iii) accessed the information in a manner consistent with her duties as a custodian or affiliate and not for an improper purpose; and (iv) did not use or disclose the information, except to determine that she had accessed the information in error and to destroy the information.
There are other relevant factors	Applicable	The custodian is aware that Dr. Jones immediately destroyed the information after determining she was not the intended recipient.

As Dr. Jones was not the individual who was intended and authorized to receive the disclosure, this is an example of unauthorized disclosure.

Part A Assessment:

- 8.1(1)(a). There is a reasonable basis to believe that a person has accessed or will be able to access the health information.
- 8.1(1)(c). There is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud.
- 8.1(1)(d). 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.
- 8.1(1)(e) There is a reasonable basis to believe that a health service was adversely affected.

As one or more factors in Part A are applicable, notification may be required.

Part B Assessment:

- 8.1(1)(i). The custodian can demonstrate that the information has been accessed and that the only person who accessed the information or to whom the information was disclosed:
  - is a custodian or affiliate;
  - is subject to confidentiality policies and procedures that meet the requirements of section 60 of the Act;
  - accessed the health information in a manner consistent with the person's duties as a custodian or affiliate and not for an improper purpose; and
  - did not use or disclose the information beyond determining that the access or disclosure was in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure.
- The custodian has considered other relevant factors.

As one or more of the factors in Part B is applicable, the risk is appropriately mitigated and notification is not required.

While the notification requirements under **section 60.1 of the *Health Information Act*** are not triggered in this incident, notification should still be considered due to the resulting delay in the delivery of health services. The custodian should consider notifying the treating health services provider and/or the patient.

NOTIFICATION IS NOT REQUIRED but should be considered.

Risk of Harm Assessment Example 7 – Loss:

A physician at an Alberta hospital took home a laptop containing a copy of the health information of about 200 of her patients. Her home was broken into and the laptop was stolen. The laptop was not encrypted or password-protected, and was not be recovered.

In this case, the physician (an affiliate of the regional health authority) is the individual who caused the loss. The regional health authority is the custodian responsible for assessing the risk of harm in this incident.

Part A: Circumstances where Notification is required		
Factor	**Applicable/Not Applicable**	**Rationale**
8.1(1)(a) whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;	Applicable	There is a reasonable basis to believe that this information has been or may be accessed, as any person will be able to access the information because the laptop was not encrypted or password-protected.
8.1(1)(b) whether there is a reasonable basis to believe that the information has been misused or will be misused;	Applicable	The circumstances surrounding the incident provide a reasonable basis to believe that the incident was deliberate. Hence, there is a greater likelihood the health information involved has been or will be misused. The information contained in the laptop includes diagnostic, treatment and care information as well as registration information, both of which is of a type of information that could be misused.
8.1(1)(c)	Applicable	The circumstances surrounding the incident and the information contained in the laptop which includes diagnostic,

whether there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud;		treatment and care information as well as registration information, provide a reasonable basis to believe that the information could be used for identity theft or to commit fraud.
8.1(1)(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;	Applicable	The information contained in the laptop could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual(s).
8.1(1)(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;	Applicable	The loss has not and will not adversely affect the provision of health services to the affected individuals, as the original records are still the possession of the hospital.
There are other relevant factors	Applicable	The custodian is aware that this loss was a result of criminal activity (theft), but it is unclear whether or not the laptop was stolen for the purposes of misusing the information on it. Nonetheless, the manner of the loss may indicate that if the information is discovered, it is more likely to be used for criminal purposes.

Part B: Circumstances where notification is not required		
Factor	**Applicable/ Not Applicable**	**Rationale**
8.1(1)(f) in the case of electronic information, whether the custodian is able to 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;	Not Applicable	The information was not secured in a manner or form that would prevent the information from being accessed or that would make the information inaccessible or unintelligible to an unauthorized person.
8.1(1)(g) in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was (i) destroyed, or (ii) rendered inaccessible or unintelligible;	Not Applicable	The information was not lost in a manner that would destroy the information or render it inaccessible or unintelligible.

8.1(1)(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;	Not Applicable	In this case, this factor is not relevant as this is not an incident of loss where the information has been recovered.
8.1(1)(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	Not Applicable	In this case, this factor is not relevant as this is not an incident of unauthorized access or disclosure.

by or disclosed to the person in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure.		
There are other relevant factors	Not Applicable	The custodian is not aware of any other relevant factor that would mitigate a risk of harm.

Information that 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. Therefore, this incident is an example of loss.

Part A Assessment:

- 8.1(1)(a). There is a reasonable basis to believe that any person has accessed or will be able to access the health information.
- 8.1(1)(b) & 8.1(1)(c). There is a reasonable basis to believe that the health information will be misused or has been misused and that the health information could be used for identity theft or committing fraud.
- 8.1(1)(d). 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.
- The custodian has considered other relevant factors.
- As one or more factors in Part A are applicable, notification may be required.

Part B Assessment:

As none of the factors from Part B are applicable, notification is required.

NOTIFICATION IS REQUIRED

Things to Consider

Where there is a risk of harm to an individual who is not the subject of the information, the *Health Information Act* **does not require** the custodian to notify the Commissioner, Minister or individual. A custodian may still wish to consider where a breach might pose a risk of harm to an individual other than the subject of the information, and may still notify in such a situation if they so choose.

Similarly, a custodian may wish to inform an individual of any risk of harm that may exist to them from a situation which does not involve a breach, such as if a dosage is incorrect on a prescription.

14.7 Notification

If a custodian believes, as a result of their investigation and assessment, that there is a risk of harm to an individual as a result of a loss, unauthorized access or disclosure, the custodian **must** notify the Commissioner, Minister and individual(s) who are the subject of the individually identifying health information (affected individual(s)) as soon as practicable.

The notice to the Commissioner, Minister or affected individual(s) should not contain any individually identifying information, other than the information necessary to contact the responsible custodian and the individual's contact information as part of the notification to the affected individual.

The notice to the Commissioner, Minister, and affected individual(s) is intended to be executed at the same time; however, as a copy of the notice to the individual must be included in the notice to the Commissioner, the notice to the individual must be prepared first. The notice to the affected individual may precede the notice to the Commissioner and the Minister, if the custodian believes the circumstances warrant urgent notice to the individual. This may also be the case where the loss, unauthorized access or disclosure was brought to the attention of the custodian by the affected individual, such as where an individual discovers an unauthorized access through the review of their Alberta Netcare Audit Log.

Notice to the Commissioner and the Minister may precede the notice to the individual where the custodian is requesting approval for substitutional notice to the individual.

A substitutional notice is served when notice cannot directly be given to the affected individual(s) or when doing so would be impractical and might not be effective. Examples of substitutional notices include television commercials and newspaper ads. Where a number of individuals have been impacted by a breach, notification to the individuals must be completed by notifying each individual separately, unless substitutional service is approved. Notification to the Commissioner and the Minister regarding the same breach affecting numerous individuals can be completed by submitting the **Notification to the Commissioner Form** and the **Notification to Alberta's Minister of Health Form** once to the appropriate office. The number of individuals to whom there is a risk of harm must be identified on the notice.

14.7.1 Notification to Affected Individual(s)

Where a custodian has determined that a risk of harm exists as a result of the loss, unauthorized access, or disclosure of individually identifying health information in the custody or control of the custodian, the custodian must, as soon as practicable, notify the affected individual in a method authorized by **section 103 of the *Health Information Act*** and must include the content prescribed by **section 8.2(4) of the *Health Information Regulation***.

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 to the individual, the custodian may decide not to notify the individual.

Where the custodian decides not to notify the individual, the custodian must immediately give notice to the Commissioner of his or her decision as in accordance with **section 8.3 of the *Health Information Regulation***.

- Notification of this decision is to be must be submitted in writing to the Commissioner in a form approved by the Commissioner, with the completed. **Notification to the Commissioner Form**. The link to this form can be found on the Checklist for Notification to the Commissioner in Appendix 3..
- The notification must set out the total number, or if the number cannot be determined, an estimate of the number of individuals that the custodian expects not to notify.

The Commissioner has the power to order the custodian to notify affected individuals, and the custodian must comply with this order.

Notification Form and Content

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

Note: Please ensure that there is no individually identifying information in the notification, other than the information that is necessary to identify the custodian who is providing the notification. The identity of the individual who is the subject of the information and the identity of the individual who is responsible for the loss, unauthorized access or disclosure should not be readily ascertainable from the notification.

(a) a description of the circumstances of the loss or unauthorized access or disclosure;
(b) the date on which or period of time within which the loss or unauthorized access or disclosure occurred;

(c) the name of the custodian who had custody or control of the health information at the time of the loss or unauthorized access or disclosure,
(d) a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure;
NOTE: Where a loss or unauthorized access or disclosure has occurred, and the custodian is not sure of the specific information that was lost or accessed or disclosed without authorization, the custodian should indicate the types that they are sure have been lost or accessed or disclosed. Additional information that may have been involved can also be included if the custodian considers it to be relevant.
(e) a description of the risk of harm to the individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed;
(f) 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;
(g) 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 a future loss or unauthorized access or disclosure;
(h) 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;
(i) a statement that the individual may ask the Commissioner to investigate the loss or unauthorized access or disclosure that includes contact information for the Office of the Information and Privacy Commissioner;
(j) the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure; and
(k) any other information that the custodian considers relevant.

The **Checklist for Notification**, found in **Appendix 3**, can assist custodians in ensuring they have met all of the notification requirements.

Where the loss, unauthorized access or disclosure involves information that could be used for fraud or identity theft, custodians may wish to include in the notice information on how to contact credit card providers and credit reporting agencies so as to monitor the individual's accounts.

Substitutional Service

Where notifying an individual directly would result in ineffective notification the custodian may apply to the Commissioner for permission to notify affected individuals by substitutional service. Situations where substitutional service may be appropriate include where the number of affected individuals is large, where the custodian does not have current contact information for the

affected individuals, or where the loss, unauthorized access or disclosure was a result of contacting the individual at his or her last known address.

To request substitutional service, the custodian should indicate this in the appropriate section of the **Notification to the Commissioner Form**, and provide his or her rationale for the request.

Examples of substitutional service include:

- A newspaper ad
- A poster in the custodian's public waiting area
- A television commercial
- A notice on the custodian's website

Example of Direct Notice to an Individual:

Ozero Clinic Inc. File #12334

March 4, 2015

Ms. Jessica Concordance
29 Agogo Close
Edmonton, Alberta
T2T 2T2

Dear Ms. Concordance,

We regret to inform you that there has been an unauthorized access to your health information. On February 28, 2015, an employee of Dr. Steven Jones inappropriately accessed your diagnostic, treatment and care information contained in Netcare (the Alberta Electronic Health Record).

This notice is being provided to you in accordance with the requirement to notify an individual of an unauthorized access to their health information under section 60.1 of the *Health Information Act,* and as a precautionary measure to prevent or reduce possible risk of harm to you.

The type of information accessed by the employee was the results of your laboratory tests. We have conducted a risk of harm assessment and determined that as this type of information had the potential to cause harm, such as embarrassment, there is a potential for misuse.

Disciplinary action against the employee is being considered and the employee's access to Netcare has been revoked. To prevent such actions from occurring in the future, Ozero Clinic is requiring all employees to retake privacy and security training which will address the appropriate use of Alberta Netcare.

If you have concerns regarding the privacy and security of your information in Netcare, we would recommend you obtain a copy of your Netcare Audit Log. This log will show the names of any individual who has accessed your Alberta Netcare record, the date this access occurred and the activities the individual undertook while in your record. A Netcare Audit Log can be obtained by contacting the Alberta Health Freedom of Information and Protection of Privacy Office at 780-422-5111.

Please be advised that the Information and Privacy Commissioner 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 Office of the Information and Privacy Commissioner at 780-422-6860 (Toll-free at 1-888-878-4044) or generalinfo@oipc.ab.ca.

If you have questions regarding this incident or notice, please feel free to contact me at 780-000-0000 or erindayo.smith@ozero.ca.

Thank you,

Erindayo Smith

Privacy Officer
Ozero Clinic Inc.
10 Dancing Street
Edmonton, Alberta
T5N 1L6
Email: erindayo.smith@ozero.ca
Phone: 780-000-0000

Example of Substitutional Notification – Newspaper Notice or Notice on Custodian's Website:

March 6, 2015

Public Notice of a Breach of Health Information

To all current and past patients of the Calgary Eye Clinic,

On February 28, 2015, the computer network of the Calgary Eye Clinic, under the custodianship of Dr. Janine Decker, was hacked. We regret to advise that the health information of about 1 million patients may have been exposed to the hacking attack. Individuals who have received treatment at the Calgary Eye Clinic between January 1, 2008 and December 31, 2015 may have been affected by this incident. This notice is being provided in accordance with section 60.1 of the *Health Information Act*.

Information that may have been exposed as a result of this incident includes registration information such as: patient name, ethnicity, marital status, dependents' information, phone number and email. It also includes Personal Health Numbers, drivers' license and credit card numbers.

Due to the potential for misuse of the type of information involved in this incident, we believe that the individuals whose information has been exposed may be at risk of identity theft or fraud, potentially resulting in financial loss.

To determine if your information was involved in this incident, please call the clinic's toll-free number at 1-800-222-4444.

Additionally, you may call your credit card company and follow the directions given to you in order to protect yourself from identity theft. You may also contact the credit reporting companies at 1-800-000-0000 or 1-877-111-1111 and advise them of this incident, if your information is involved. Affected individuals are advised to monitor their financial account and immediately contact their respective financial institutions or credit card companies if they notice any discrepancies.

The Calgary Eye Clinic is working in conjunction with the Information and Privacy Commissioner, credit card companies, credit-reporting agencies and the RCMP to resolve this issue and reduce any potential risk of harm to our patients identified above.

The Personal Health Number allows individuals to receive publicly funded services paid for by the Alberta Health Care Insurance Plan, such as doctor's check-ups. A Personal Health number can be monitored by requesting a Statement of Benefits Paid from Alberta Health. To request a Statement of Benefits Paid, please contact Alberta Health at 310-0000 or in Edmonton at 780-644-7551.

The Calgary Eye Clinic has taken immediate steps to strengthen its IT security controls and is considering long-term options for improvements to its internationally accredited computer security system that was in place prior to the hacking incident.

Please be advised that the Information and Privacy Commissioner 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 Office of the Information and Privacy Commissioner at 780-422-6860 (Toll-free at 1-888-878-4044) or generalinfo@oipc.ab.ca.

Individuals requesting further information regarding this notice should contact the Calgary Eye Clinic Privacy Officer at 1-800-222-0000.

For media enquiries, please contact the Calgary Eye Clinic Director of Public Affairs and Communications at 780-000-0000.

14.7.2 Notification to Commissioner

Notification to the Commissioner must be in a form approved by the Commissioner. The link to the **Notification to the Commissioner Form** is found on the Checklist for Notification to the Commissioner in **Appendix 3**.

To meet the requirement to notify the Commissioner, part A of the **Breach Reporting Form** must be completed in full and provided to the Commissioner at the contact information listed on the form. The custodian may wish to keep the original form on file, and send copies of the form to the Commissioner.

Notice to the Commissioner must include all of the following information, as prescribed by **section 8.2(2) of the *Health Information Regulation***, as well as any additional information the custodian determines to be relevant:

Note: Please ensure that there is no individually identifying information in the notification, other than the information that is necessary to identify the custodian who is providing the notification. The identity of the individual who is the subject of the information and the identity of the individual who is responsible for the loss, unauthorized access or disclosure should not be readily ascertainable from the notification.

(a) the name of the custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure;
(b) a description of the circumstances of the loss or unauthorized access or disclosure;
(c) the date on which or period of time within which the loss or unauthorized access or disclosure occurred;
(d) the date on which the loss or unauthorized access or disclosure was discovered;
(e) a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure;
(f) a non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed that includes a non-identifying description of the custodian's consideration of the factors referred to in section 8.1(1), including any relevant factors not detailed in that section;
    - *This description should be in enough detail that the Commissioner can understand which risk factors have been assessed and are applicable in this circumstance.*
(g) the number, or if the 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;
(h) 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;
(i) 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 a future loss or unauthorized access or disclosure;
(j) a non-identifying copy of the information that has been or will be provided in the notice to the individual who is the subject of the individually identifying health information referred to in **section 8.2(4) of the *Health Information Regulation***, if applicable, together with a statement indicating the method referred to in **section 103 of the *Heath Information Act*** that has been or will be used to give notice to the individual, if applicable;
    - *Where the custodian is requesting substitutional service or has determined that providing notification to the individual would result in a risk of harm, a copy of the notice that would be provided to the individual is not required.*

(k) if the custodian is requesting the authorization of the Commissioner to give notice to an individual by substitutional service under **section 103(c) of the *Health Information Act***, the request together with a statement of the reasons for the request;
(l) the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure; and
(m) any other information that the custodian considers relevant.

The **Checklist for Notification**, found in **Appendix 3**, can assist custodians in ensuring they have met all of the notification requirements. An example of a completed notification form is also found in **Appendix 3**.

14.7.3 Notification to the Minister

Notification to the Minister must be in a form approved by the Minister. The link to the **Notification to Alberta's Minister of Health Form** is found on the Checklist for Notification to the Minister in **Appendix 3**.

To meet the requirement to notify the Minister, part B of the **Breach Reporting Form** must be completed in full and provided to the Minister at the contact information listed on the form. The custodian may wish to keep the original form on file, and send copies of the form to the Minister.

Notice to the Minister must include all of the following information, as prescribed by **section 8.2(3) of the *Health Information Regulation***:

Note: Please ensure that there is no individually identifying information in the notification, other than the information that is necessary to identify the custodian who is providing the notification. The identity of the individual who is the subject of the information and the identity of the individual who is responsible for the loss, unauthorized access or disclosure should not be readily ascertainable from the notification.

(a) the name of the custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure,
(b) a description of the circumstances of the loss or unauthorized access or disclosure,
(c) a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure,
(d) a non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed that includes a non-identifying description of the custodian's consideration of the factors referred to in section 8.1(1), including any relevant factors not detailed in that section,

(e) the number, or if the 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,
(f) 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,
(g) the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure, and
(h) any other information that the custodian considers relevant.

The **Checklist for Notification**, found in **Appendix 3**, can assist custodians in ensuring they have met all of the notification requirements. An example of a completed notification form is also found in **Appendix 3**.

14.8 Compliance with the Duty to Notify

To ensure compliance with the duty to notify, a custodian should consider the following steps:

1. Designation of Affiliate Responsible for Compliance with Duty to Notify
2. Creation of a Duty to Notify Policy
3. Organizational Awareness of Requirements and Policy/Process
4. Audit and Update of Organizational Procedures

14.8.1 Designation of Affiliate Responsible for Compliance with Duty to Notify

Within a custodian's organization, a custodian should designate a specific affiliate or affiliates who are responsible for meeting the requirements of **section 60.1 of the *Health Information Act***. Depending on the needs of the organization, options include the custodian, a single affiliate, or multiple affiliates. Throughout this chapter, we will refer to this individual as the **responsible affiliate**.

Any affiliate of the custodian may be designated as the responsible affiliate. This could be a clinic manager, clerk, nurse, physician or a clinic privacy officer responsible for compliance with the *Health Information Act*.

Some large custodian organizations, such as those with multiple facilities, may require multiple responsible affiliates, one being the central privacy office. However, any one of the responsible affiliates in the multiple responsible affiliate organization should have the authority to administer the prevention and management of an incident within their area of practice or control. For

example, the responsible affiliate for a hospital department may notify a central responsible affiliate in the hospital's main privacy office, but the department's responsible affiliate is able to independently make decisions on risk mitigation and notification for each incident.

Where the custodian's policy designates an affiliate as responsible for compliance with the duty to notify, an affiliate's notification to the responsible affiliate is deemed as a notice to the custodian and the affiliate has met its duty under **section 60.1(1) of the *Health Information Act***.

14.8.2 Policies and Procedures

In accordance with **section 63 of the *Health Information Act***, a custodian must have in place policies and procedures that will assist in the administration of the Act, including a policy for responding to a loss, unauthorized access or disclosure. When creating a policy regarding compliance with the duty to notify, or updating an existing policy, a custodian should consider any existing policies and procedures they have in place with regards to mitigation, incident response, or notification.

A policy should include the following information, as well as any additional information the custodian deems relevant:

A statement regarding the purpose of the policy;

- Who the policy applies to;
- Steps the custodian will take to be in compliance with **section 60.1 of the *Health Information Act***; including, but not limited to:
    - How affiliates will comply with the requirement to notify the custodian of any loss, unauthorized access or disclosure;
    - How the custodian will assess risk;
    - How the custodian will notify the Commissioner, Minister, and any affected individual(s), where applicable;
- How the custodian will contain and mitigate any loss, unauthorized access or disclosure;
- If any exceptions apply to the policy;
- Who within the custodian organization is responsible for:
    - Reviewing and updating the policy;
    - Receiving notifications from affiliates;
    - Containment and mitigation strategies;

    - Assessing risk of harm;
    - Notification to Minister, Commissioner and affected individual(s), where required;
- Any requirements on the custodian to notify other entities of an incident (such as a regulatory body or law enforcement agency);
- Any penalties or consequences set either by the *Health Information Act* or by the custodian for failing to meet the policy requirements;
- The date the policy is effective;
- Contact information for someone within the custodian's organization who can answer an affiliate's questions about the policy; and
- References or links to any applicable resources to assist with understanding or complying with the policy (e.g. a link to the **Breach Reporting Form**, or where applicable, the organization's form for reporting a loss, unauthorized access or disclosure by an affiliate).

14.8.3 Organizational Awareness of Requirements and Policy/Procedures

In order to ensure that a custodian is meeting the requirements of the duty to notify, the custodian should ensure that all affiliates are sufficiently aware of their responsibilities. Examples include:

- Providing education about affiliates' responsibilities under the new notification requirement under **section 60.1 of the *Health Information Act***;
- Training affiliates on the custodian's notification policy;
- Providing education to affiliates on incident prevention and mitigation;
- Educating affiliates on the existence of internal and external audit functions, monitoring and tracking mechanisms in respect to the organization's handling of health information;
- Referring affiliates to internal policies, or to publicly available resources, on the new reporting requirement;
- Conducting a response to a mock incident to assess the organization's preparedness to respond to a real incident;
- Assessing preparedness by using lessons learned from previous responses to actual incidents;
- If applicable, ensuring that the organization's web resources are updated with the new requirements; and

- Providing links to relevant web-based resources regarding the new requirement on the custodian's website(s).

14.8.4 Audit and Update of Organizational Procedures

The June 2014 amendments to the *Health Information Act* also make it an offence to fail to take reasonable steps in accordance with the 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 of loss of health information. As such, custodians should regularly conduct an audit of their internal procedures and safeguards and update them as necessary. This may include:

- Reviewing administrative, physical, and technical controls for the protection of health information;
- Reviewing existing monitoring, tracking, and response procedures;
- Consulting with other staff to update records and information management policies with the new notification requirements;
- Reviewing internal collection, use and disclosure practices, as well as practices regarding the secure destruction of records; and
- Establishing a schedule for reviewing administrative, technical and physical safeguards.

Ensure these practices and policies are in alignment with the *Health Information Act*, and update as necessary.

14.9 Responding to a Loss, Unauthorized Access or Disclosure

In addition to a notification policy, custodians should also have a procedure in place for responding to a loss, unauthorized access or disclosure within their organization. Some areas of this procedure may overlap with the notification policy, or the policy may direct affiliates to the procedure.

An incident response procedure should address the following six steps for responding to a loss, unauthorized access or disclosure within the custodian's organization:

1. Initiate organizational incident response procedure

The affiliate who becomes aware of the loss, unauthorized access or disclosure should notify the custodian or responsible affiliate as per the custodian's policy and **section 8.2(1)** of the *Health Information Regulation*.

- Steps may include:
    - Notifying the custodian, in accordance with the custodian's policies and procedures, that a loss, unauthorized access or disclosure has occurred.
    - Ensuring that notice is also available in written format, notwithstanding the manner in which notice is provided to the custodian.
        - For example, supplement a phone call with an email or a record of the phone call.
    - Confirming that the custodian has received the notice.
        - For example, follow up on a voicemail message left for the custodian or request a "read receipt" when sending email to the custodian.

2. Contain the incident & mitigate risk

The custodian should attempt to contain the loss, unauthorized access or disclosure to prevent any further risk of harm. This may include recalling a misdirected email or fax, attempting to retrieve misplaced files, or shutting down an area of weakness within the computer's security system. Depending on the custodian's incident response procedure, affiliates may be required to take some containment steps before receiving direction from the custodian. This may be the case where immediate action could help to mitigate risk, such as where an affiliate immediately realizes that they have sent an email to the wrong address. In circumstances such as this, the custodian's policy or procedure may direct them to attempt to recall the message immediately, before notifying the custodian.

An incident response procedure may require:

- Contacting support personnel (such as IT staff) needed to assist with containment.
- Notification of affected individuals immediately if immediate notice will help reduce risk of harm to them.
    - **Note**: At this point, the custodian may not have all the information required by the regulations, therefore a second notification to the affected individual may be necessary if this immediate notice does not meet the requirements.

- Facilitation of notification to relevant health professionals if, for example, the loss or theft of health information may jeopardize the delivery of urgently needed health services to an individual (for example, if a test result is lost and the individual requires immediate health care based on the outcome of that test result).
- Consideration as to whether creating a general awareness within the organization is necessary for containing the loss, unauthorized access or disclosure.
- Participation of relevant staff within the organization in the containment and investigation of the loss, unauthorized access or disclosure.
    - For example, in the case of a lost laptop, the support of other staff may be needed to find it.
- An initial incident report to be used in notification (as applicable) to:
    - Internal authorities, e.g. the custodian, legal counsel, communications team;
    - Other organizations based on contractual obligations; and/or
    - The police if the loss, unauthorized access or disclosure involves theft or criminal activity.

3. Investigate the loss, unauthorized access, or disclosure

The custodian should investigate the loss, unauthorized access or disclosure of individually identifying health information. This should include identification of:

- The cause of the loss, unauthorized access or disclosure (e.g. was this a case of an affiliate snooping? A lost access card? A misdirected fax? A hacking incident?);
- The root cause of the loss, unauthorized access or disclosure (e.g. did the affiliate snoop because they were unaware of the custodian's policies? Was the hacking able to take place because the security safeguards were insufficient?);
- Whether the loss, unauthorized access or disclosure was intentional or accidental;
- Whether the loss, unauthorized access or disclosure could have been avoided;
- The date and time, or time period of the loss, unauthorized access or disclosure;
- The date the loss, unauthorized access or disclosure was discovered;
- The types of information involved in the loss, unauthorized access or disclosure;
- The safeguards that were in place at the time of incident;
- An estimate or exact number of individuals who may be affected by the loss, unauthorized access or disclosure;

- Any initial steps the custodian has taken to contain the loss, unauthorized access or disclosure and mitigate risk to those involved;
- Whether the loss, unauthorized access or disclosure was an isolated incident or indicates systemic issues; and
- Which affiliates or service providers were involved or impacted by the breach.

  The custodian should exercise discretion to ensure that the process of containment or risk assessment does not result in any further loss, unauthorized access or disclosure.

- For example, the custodian should refrain as much as possible, from revealing any information that could lead to the identification of the individual whose health information has been lost, accessed or disclosed inappropriately.
- In addition, unless otherwise needed for the success of the investigation, containment, or risk assessment and notification, making the identity of the person responsible for the loss, unauthorized access or disclosure known to the general staff should be avoided.

4. Assess for risk of harm

The custodian must assess whether there is a risk of harm to an individual as a result of a loss, unauthorized access or disclosure of individually identifying health information.

- This assessment must be done in consideration of the factors set out in **section 8.1(1) of the *Health Information Regulation***, as well as any other factor(s) the custodian deems relevant.
- Based on all available information, the custodian must determine whether a risk of harm exists to an individual.
- If the custodian has established that a risk of harm exists to an individual, notification to the Commissioner, Minister and any affected individual(s) is required.

  Section 14.6 and Appendix 3 of the HIA Guidelines and Practices Manual refer to more information on assessing risk of harm.

5. Notify (if required)

Where the custodian determines that there is a risk of harm to the individual who is the subject of the information as a result of the loss, unauthorized access or disclosure of individually identifying health information in the custody or control of the custodian, the custodian must notify the Minister, Commissioner, and any affected individual(s) in accordance with the regulations as soon as practicable. If the individual was notified as part of the containment or risk mitigation process,

and the notification met all the requirements of the regulations, a secondary notice to the individual is not required.

Where there is a risk of harm to an individual who is not the subject of the information, the custodian should consider whether notification to that individual or another individual is necessary to appropriately mitigate that risk.

Section 14.7 and Appendix 3 of the HIA Guidelines and Practices Manual provide more information on notification.

6. Monitor, Track, and Learn

After a loss, unauthorized access or disclosure of individually identifying health information has been contained, the custodian should, as appropriate:

- Prepare an Investigation Report for internal documentation, which should include:
    - A summary of the incident;
    - The immediate response taken to contain the loss, unauthorized access or disclosure and reduce harm;
    - Background of the incident;
        - Timelines;
        - Type(s) of information involved;
    - Description of the investigative process;
    - Summary of interviews held (internally and externally);
    - A review of safeguards and protocols;
    - Summary of possible solutions and recommendations;
    - Description of necessary remedial actions, including short and long term strategies to correct the situation;
    - Detailed description of next steps;
    - Responsibility for implementation and monitoring, including timelines;
        - May also include the names and positions of individuals responsible for implementation.
- Monitor the situation for any future risks;

- Provide the Minister with further clarification on the loss, unauthorized access or disclosure that has been reported, if requested;
- Respond to further enquiries by the Commissioner and cooperate with the Commissioner in conducting investigations, where applicable;
- Respond to requests for further explanations or clarifications from any affected individual(s).
    - Consider recommending appropriate disciplinary actions against persons responsible in accordance with **section 8(7) of the *Health Information Regulation***;
    - Determine whether this loss, unauthorized access or disclosure is systemic in nature and, if so, consider what needs to be done to stop it;
    - Determine measures that may need to be put in place to prevent this type of loss, unauthorized access or disclosure from occurring again;
    - Consider conducting a review of the organization's information security practices, including updates to physical, administrative, and technical controls, where necessary;
    - Consider whether the loss, unauthorized access or disclosure and decisions made in respect of it, are a learning opportunity for the organization as a whole and coordinate efforts to disseminate this learning to the organization in a way that prevents further incidents; and
    - Retain investigation results via a secure tracking method.

14.10 Prevention

To help prevent a loss, unauthorized access or disclosure from occurring, it is recommended that custodians:

- Complete Privacy Impact Assessments (PIAs) as required and ensure existing PIAs appropriately identify risks and risk mitigation strategies;
- Train and educate affiliates as well as information managers on legislative responsibilities and internal policies;
- Understand collection, use and disclosure authorities;
- Only collect, use, and disclose the least amount of information necessary with the highest degree of anonymity;
- Ensure that information manager agreements, research agreements, and contracts include discussion of privacy and security requirements and specific instructions regarding the custodian's breach policy;

- Establish a schedule for conducting regular reviews of safeguards, policies, and procedures;
- Ensure policies are up to date and reflect organizational needs;
- If possible, refrain from putting individually identifying health information on portable devices;
- Ensure mobile devices containing individually identifying health information are password protected and encrypted;
- Confirm policies and procedures are in place that ensure the protection of the health information that is in the custody or under the control of the custodian (including, but not limited to collection, use and disclosure, destruction of records, storage);
- Have in place administrative, technical, and physical safeguards to protect health information. For example, locked cabinets, password protection, or access card entry to secure areas);
- Ensure that any electronic medical record has in place logging and auditing capacity, that regular auditing takes place, and that staff are aware that these audits and logs are in place; and
- Consult with legal and privacy teams.

14.11 Offences and Penalties

Under the *Health Information Act* there are numerous offence provisions related to the duty to notify. It is an offence:

- for a custodian to fail to take reasonable steps in accordance with the 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;
- for a custodian to fail to notify the Commissioner, Minister and affected individual where there is a risk of harm to an individual as a result of a loss, unauthorized access or disclosure;
- for a custodian to fail to consider all appropriate factors when assessing risk of harm;
- for a custodian who does not notify the Commissioner, after deciding not to notify an individual;
- for a custodian to fail to comply with an order of the Commissioner requiring the custodian to provide notice to an individual; and
- for an affiliate to fail to notify the custodian where the affiliate becomes aware of a loss, unauthorized access or disclosure of health information.

Pursuant to **section 107 of the *Health Information Act***, fines for these offences could range from $2,000 to $10,000 (in the case of an individual) and from $200,000 to $500,000 (in the case of any other person).

Things to Remember

Duty to Notify

What is a Loss, Unauthorized Access or 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. This may involve a physical or electronic loss of records in contravention of the Act.
- An unauthorized access occurs where an individual accesses information that they were not authorized to access.
- An unauthorized disclosure occurs where there has been a deliberate or accidental disclosure of information in contravention of the *Health Information Act*.

What are my Duties as a Custodian?

- Where a custodian becomes aware of a loss, unauthorized access or disclosure of individually identifying health information, the custodian must assess whether there is a risk of harm to an individual as a result of the loss, unauthorized access or disclosure.
- Where the custodian determines that there is a risk of harm, the custodian must notify, as soon as practicable, the Commissioner, Minister, and any affected individual(s), in accordance with the regulations.
- If a custodian considers that giving notice to an individual who is the subject of individually identifying health information that has been breached could reasonably be expected to result in a risk of harm to the individual's mental or physical health, the custodian may decide not to give notice to the individual. If the custodian decides not to give notice to the subject, then the custodian must immediately give notice to the Commissioner of their decision not to give notice to the individual. Such a notice to the Commissioner must include the reasons for this decision, in accordance with the regulations.

What are my Duties as an Affiliate?

- Where an affiliate becomes aware of a loss, unauthorized access or disclosure of individually identifying health information, the affiliate must, as soon as practicable, notify the responsible custodian in accordance with **section 8.2(1) of the *Health Information Regulation***.

What is the Level of Risk Requiring Notification?

A level of risk requiring notification exists where:

- 8.1(1)(a) there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;
- 8.1(1)(b) there is a reasonable basis to believe that the information has been misused or will be misused;
- 8.1(1)(c) there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud;
- 8.1(1)(d) 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;
- 8.1(1)(e) 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;
- There are other relevant factors that could result in risk of harm.

The risk of harm has been appropriately mitigated, and notification is not required where:

- 8.1(1)(f) in the case of electronic information, the custodian is able to 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;
- 8.1(1)(g) in the case of a loss of information, the custodian is able to demonstrate that the information was lost in circumstances in which the information was
    i. destroyed, or
    ii. rendered inaccessible or unintelligible;
- 8.1(1)(h) in the case of a loss of information that is subsequently recovered by the custodian, the custodian can demonstrate that the information was not accessed before it was recovered;

- 8.1(1)(i) in the case of an unauthorized access to or disclosure of information, 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.
- There are other relevant factors that would mitigate the risk.

Appendix 1 - Forms

Notification to Alberta's Minister of Health Form

The Notification to Alberta's Minister of Health Form can be found at: http://www.health.alberta.ca/about/Health-Information-Act.html.

Notification to the Commissioner Form

The Notification to the Commissioner Form can be found at: https://www.oipc.ab.ca/forms.aspx.

Appendix 2 – Model Letters:

Notice of Loss, Unauthorized Access or Disclosure

[C*ustodian's file reference number*]

[D*ate*]

[N*ame and address of affected individual*]

Dear [*Title and name of affected individual*],

This notice is to advise you that your health information that was in the custody and control of [*name of custodian*] was [*type of incident: lost/inappropriately accessed/disclosed inappropriately*].

The information involved in the [*type of incident: loss, unauthorized access or disclosure*] was [*type(s) of health information involved*] held by [*custodian name*].

The incident occurred on [*date or time period of incident*] when [*describe the circumstances of the loss, unauthorized access or disclosure*].

This notice is being provided to you in accordance with the requirement to notify of a *[type of incident: loss, unauthorized access or disclosure]* under section 60.1 of the *Health Information Act* and as a precautionary measure to prevent or reduce possible risks of harm to you as a result of the *[type of incident: loss, unauthorized access or disclosure]*.

[*Custodian*] has determined that, as a result of this incident, there may be a risk of [*description of harm*] to you because [*how the risk of harm was assessed*]. We have taken the following steps to reduce the risk of harm to you: [*description of steps taken to reduce the risk of harm*]. We will be taking further steps to reduce the risk of harm, including [*description of additional steps that will be taken*]. To prevent this incident from occurring in the future, we are [*description of steps that will be taken to prevent future occurrence*].

We strongly suggest that you [*description of steps the individual may take to reduce the risk of harm*].

Please be advised that the Information and Privacy Commissioner 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 Office of the Information and Privacy Commissioner at 780-422-6860 (Toll-free at 1-888-878-4044) or generalinfo@oipc.ab.ca.

If you require further information or you have questions regarding this notice, please feel free to contact [*name of custodian or responsible affiliate*] at [*phone number and/or email address*].

Sincerely,

[Name of custodian or responsible affiliate]

[Position title for custodian or responsible affiliate]

Appendix 3 – Responsibilities of Custodians

Risk of Harm Checklist

In accordance with section 60.1 of the *Health Information Act* (HIA) and section 8.1 of the *Health Information Regulation*, when any individually identifying health information under the custody or control of a custodian is lost, or there is an unauthorized access to or disclosure of individually identifying health information, the custodian must evaluate the risk of harm to the individual who is the subject of that information in determining whether or not to proceed with notification to that individual, the Information and Privacy Commissioner, and the Minister of Health. When determining the risk of harm, the custodian must consider the following factors:

Section 1

- Is there reason to believe that the information has been or may be accessed by or disclosed to a person? Yes ☐ No ☐
- Is there reason to believe that the information has been misused or will be misused? Yes ☐ No ☐
- Is there reason to believe that the information could be used for the purpose of identity theft or to commit fraud? Yes ☐ No ☐
- Is there 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? Yes ☐ No ☐
- Is there 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? Yes ☐ No ☐
- Are there any other factors that indicate a risk of harm to the individual who is the subject of the information? Yes ☐ No ☐

If you answered ‘YES’ to any of the questions above, you may be required to give notice under section 60.1(2) of the HIA. Answer the questions below to determine if the risk may have been mitigated by another circumstance.

Section 2

- 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? Yes ☐ No ☐
  - OR
  - render the information unintelligible by a person who is not authorized to access the information? Yes ☐ No ☐

- If the information was lost, can the custodian demonstrate that the information was lost in circumstances in which the information was:
  - destroyed? Yes ☐ No ☐
  - OR
  - rendered inaccessible or unintelligible? Yes ☐ No ☐

- 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? Yes ☐ No ☐

- 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: Yes ☐ No ☐
  - is a custodian or an affiliate? Yes ☐ No ☐
  - is subject to confidentiality policies and procedures that meet the requirements of section 60 of the HIA? Yes ☐ No ☐
  - 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 Yes ☐ No ☐
  - 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)? Yes ☐ No ☐

- Are there any other factors that indicate that the risk may be mitigated? Yes ☐ No ☐

If you are able to demonstrate that factors from Section 2 are present, the factors from Section 1 may be appropriately mitigated and therefore notification is not required. In some circumstances, the custodian may decide that notification is necessary even when factors from Section 2 are present.

As a custodian, you must consider if there are any other factors that are relevant which may indicate a risk of harm to the individual due to a loss of, unauthorized access to or disclosure of health information. Each situation is unique, and all factors should be considered.

For more information, contact the *Health Information Act* Help Desk
Phone: 780-427-8089 (toll free 310-0000)
Email: hiahelpdesk@gov.ab.ca

Checklist for Notification to an Individual

In accordance with section 60.1 of the *Health Information Act* and section 8.2 of the *Health Information Regulation*, a custodian must notify the individual who is the subject of the information when:

- any of the individual's individually identifying health information under the custody or control of the custodian is lost, or there is an unauthorized access to or disclosure of individually identifying health information, **AND**
- the custodian has determined that there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure.

When providing notice to an individual, the notice must be provided in writing and must include the following information:

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.

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.

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. Personal Health Number, prescription information, diagnostic imaging report, etc.). *Do not include information that could identify the affected individual (e.g., Include: "individual's Personal Health Number was disclosed". Do not include: "Individual's Personal Health Number, 99999-9999, was disclosed.").*

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 any individual**, but should include the following information:
  - ☐ The type of harm, AND
  - ☐ 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 a 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.

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 Information and Privacy Commissioner of Alberta (the Commissioner) in regards to the loss or unauthorized access or disclosure.
- ☐ Contact information for the Office of the Information and Privacy Commissioner.

For more information, contact the *Health Information Act* Help Desk
Phone: 780-427-8089 (toll free 310-0000)
Email: hiahelpdesk@gov.ab.ca

Checklist for Notification to the Minister

In accordance with section 60.1 of the *Health Information Act* and section 8.2 of the *Health Information Regulation*, a custodian must notify the Minister of Health (the Minister) when:

- any individually identifying health information under the custody or control of the custodian is lost, or there is an unauthorized access to or disclosure of individually identifying health information, **AND**
- the custodian has determined that there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure.

A custodian must notify the Minister in writing in a form approved by the Minister.

The notice to the Minister must include the following information:

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 on behalf of the custodian about the loss or unauthorized access or disclosure.

INCIDENT DESCRIPTION

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

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. Personal Health Number, prescription information, diagnostic imaging report, etc.). *Do not include information that could identify the affected individual (e.g., Include: "individual's Personal Health Number was disclosed". Do not include: "Individual's Personal Health Number, 99999-9999, was disclosed.").*

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 any individual, but should include the following information:
  - ☐ The type of harm, AND
  - ☐ An explanation of how the risk of harm was assessed that includes a non-identifying description of the factors used to assess the risk of harm.
- ☐ 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.

ADDITIONAL INFORMATION

Any other information the custodian considers relevant.

For more information, contact the *Health Information Act* Help Desk
Phone: 780-427-8089 (toll free 310-0000)
Email: hiahelpdesk@gov.ab.ca

Checklist for Notification to the Commissioner

In accordance with section 60.1 of the *Health Information Act* and section 8.2 of the *Health Information Regulation*, a custodian must notify the Information and Privacy Commissioner of Alberta (the Commissioner) when:

- any individually identifying health information under the custody or control of the custodian is lost, or there is an unauthorized access to or disclosure of individually identifying health information, **AND**
- the custodian has determined that there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure.

A custodian must notify the Commissioner in writing in a form approved by the Commissioner.

The notice to the Commissioner must include the following information:

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 on behalf of the custodian about the loss or unauthorized access or disclosure.

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.

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. Personal Health Number, prescription information, diagnostic imaging report, etc.). *Do not include information that could identify the affected individual (e.g., Include: "individual's Personal Health Number was disclosed". Do not include: "Individual's Personal Health Number, 99999-9999, was disclosed.").*

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 any individual, but should include the following information:
  - ☐ The type of harm, AND
  - ☐ An explanation of how the risk of harm was assessed that includes a non-identifying description of the factors used to assess the risk of harm.
- ☐ 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.

ADDITIONAL INFORMATION

- ☐ Any other information the custodian considers relevant.

For more information, contact the *Health Information Act* Help Desk
Phone: 780-427-8089 (toll free 310-0000)
Email: hiahelpdesk@gov.ab.ca