Office of the Information and Privacy Commissioner of Alberta

Practice Note

Reporting a Breach to the Commissioner

This practice note is for private sector organizations, health custodians and public sector bodies under the *Personal Information Protection Act*, *Health Information Act* and *Freedom of Information and Protection of Privacy Act*, respectively.

The information in this document is to help private sector organizations, health custodians and public sector bodies to notify the Information and Privacy Commissioner of Alberta (Commissioner) of a privacy breach using the **Privacy Breach Report Form.**

The information relates only to reporting a privacy breach to the Commissioner. Organizations, custodians and public bodies may have other obligations in law or otherwise regarding privacy breaches, including the duty to notify individuals affected by the privacy breach. Organizations, custodians and public bodies are responsible for making themselves aware of these obligations.

Table of Contents

Individuals should not use this form. Individuals who believe their personal or health information has been lost or improperly collected, used, disclosed or accessed by an organization, custodian or public body may file a complaint with the Office of the Information and Privacy Commissioner (OIPC) by visiting the "Request a Review / File a Complaint" webpage at www.oipc.ab.ca.

What is a Privacy Breach?

For purposes of the Privacy Breach Report Form and this document, a **privacy breach** (or breach) means a loss of, unauthorized access to, or unauthorized disclosure of personal information or individually identifying health information.

Privacy breaches can occur in a number of ways. Some of the more common incidents reported to the Commissioner include:

- Loss or theft of mobile devices (e.g. laptops, USB sticks)
- Misdirected communications (via email, fax or mail)
- Employee "snooping" of patient or customer records (also known as unauthorized access to or misuse of customer or patient information by an employee)
- Hacking of computers, servers and websites
- Malicious software ("malware") attacks, including ransomware
- Phishing or social engineering attacks
- Failure to wipe hard drives of computers and other devices prior to being resold
- Stolen paper records from an employee's vehicle, home or office
- Improper disposal of records or devices

Requirement to Report a Breach to the Commissioner

Personal Information Protection Act (PIPA)

It is **mandatory** for an **organization** with personal information under its control**,** to notify the Commissioner, without reasonable delay, of a privacy breach where:

> a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure (section 34.1).

Health Information Act (HIA)

It is **mandatory** for a **custodian** having individually identifying health information in its custody or control to notify the Commissioner, as soon as practicable, of a privacy breach if the custodian determines:

> there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure (section 60.1(2)).

In addition to notifying the Commissioner of the privacy breach, the custodian is also required by section 60.1(3) of HIA to notify the Minister of Health and the affected individuals[1] of the privacy breach.

[1] A custodian may decide not to notify an affected individual if notification could reasonably be expected to result in a risk of harm to the individual's mental or physical health. In such cases, the custodian must immediately notify the Commissioner of the decision not to notify the individual (HIA, section 60.1(5)). See Appendix A.

Freedom of Information and Protection of Privacy Act (FOIP Act)

Public bodies are not required by law to notify the Commissioner of a privacy breach; however, the OIPC advises public bodies to voluntarily report privacy breaches to the Commissioner.

Using the Privacy Beach Report Form will help a public body provide the right information to the Commissioner so that the OIPC may provide guidance to the public body for responding to the breach.

Who is Responsible for Reporting the Breach to the Commissioner?

PIPA

The organization having **control** of the personal information has the legal obligation to notify the Commissioner of a reportable breach (section 34.1).

HIA

The custodian having **custody or control** of the individually identifying health information has the legal obligation to notify the Commissioner of a reportable breach (section 60.1(2)).

An affiliate of a custodian must as soon as practicable notify the custodian of any privacy breach of individually identifying health information in the custody or control of the custodian (section 60.1(1)).

Custody vs. Control

As a general rule, information is considered to be in the **custody** of an entity when the entity has physical possession of the information.

Information is under the **control** of an entity when the entity has the authority to manage the information, including restricting, regulating and administering its use, retention and disposition, and demanding the return of the information.

An entity may not have custody of the information but still be considered to have the information under its control. For example, a contractor of an organization, custodian or public body may have custody of personal information or individually identifying health information because it has collected or created the information in relation to services performed by the contractor on behalf of the organization, custodian or public body. However, the organization, custodian or public body retains control over the information because it establishes the purposes for which the contractor may collect, use or disclose the information, directs how the information is to be secured and when it is to be disposed of, and can obtain access to the information.

Additional discussion of the criteria for establishing custody or control can be found in OIPC orders, available at www.oipc.ab.ca. See, for example, Orders F2010-022, F2010-023, F2015-21 and P2015-08.

How Quickly Does a Breach Need to Be Reported to the Commissioner?

PIPA: Organizations are required to notify the Commissioner of reportable breaches **without unreasonable delay** (section 34.1).

HIA: Custodians are required to notify the Commissioner of reportable breaches **as soon as practicable** (section 60.1(2)).

The OIPC advises that a breach be reported as soon as possible even if all the information requested on the Privacy Breach Report Form is not yet available (e.g. you have not completed your internal investigation or established long term strategies to correct the situation). Additional information can be provided to the Commissioner as it becomes known.[2]

What Information Should Be Included in the Notice to the Commissioner?

The Privacy Breach Report Form is designed to ensure organizations and custodians provide the Commissioner with the information they are required to provide under PIPA and HIA and the information the Commissioner would otherwise typically request in follow-up communications. Providing as much information up front expedites the breach reporting process.

PIPA

A notice of a breach to the Commissioner under section 34.1(1) of PIPA must include the information prescribed by section 19 of the *Personal Information Protection Act Regulation* (PIPA Regulation).

Section 19 of the PIPA Regulation states the notice must **be in writing and include the following information:**

- A description of the circumstances of the breach
- The date on which or time period during which the breach occurred
- A description of the personal information involved in the breach
- An assessment of the risk of harm to individuals as a result of the breach
- An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the breach
- A description of any steps the organization has taken to reduce the risk of harm to individuals
- A description of any steps the organization has taken to notify individuals of the breach
- The name and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the breach

[2] Under PIPA, the Commissioner will make the decision whether notification to individuals is required based on the information before the Commissioner at the time of the decision.

The Commissioner has the power to require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization to notify affected individuals or to satisfy the terms and conditions that the Commissioner may have placed on an organization that has been directed to notify affected individuals (section 37.1(4)).

HIA

A notice of a breach to the Commissioner under section 60.1(2) of HIA must be in accordance with section 8.2(2) of the *Health Information Regulation.*

Section 8.2(2) of the *Health Information Regulation* states that the notice must **be in writing in a form approved by the Commissioner and include the following information:**

- The name of the custodian who had custody or control of the information at the time of the breach
- A description of the circumstances of the breach
- The date on which or period of time within which the breach occurred
- The date on which the breach was discovered
- A non-identifying description of the type of information that was the subject of the breach
- A non-identifying description of the risk of harm to an individual as a result of the breach, including a description of the type of harm and an explanation of the 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
- 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 breach
- 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 breach
- 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 breach
- If the custodian is providing notice to affected individuals, a non-identifying copy of the information that has been or will be provided in the notice to the affected individuals referred to in section 8.2(4) together with a statement indicating the method referred to in section 103 of HIA that has been or will be used to give notice to the individuals
- If the custodian is requesting the authorization of the Commissioner to give notice to an individual by substitutional service under section 103(c) of HIA, the request together with a statement of the reasons for the request
- The name and contact information for a person who is able to answer questions on behalf of the custodian about the breach
- Any other information that the custodian considers relevant

Offences

PIPA

It is an offence for an organization to fail to notify the Commissioner of a reportable privacy breach under section 34.1 of the Act (section 59(1)(e.1)). If guilty of an offence, an individual is subject to a fine up to $10,000 and any other person to a fine up to $100,000 (section 59(2)).

HIA

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

It is an offence for a custodian:

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

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

If guilty of an offence, an individual is subject to a fine from $2,000 to $10,000, and for any other person a fine from $200,000 to $500,000 (section 107(7)).

Additional Resources

OIPC orders, investigation reports, PIPA breach notification decisions and additional information on how to respond to a privacy breach are available at www.oipc.ab.ca.

Instructions for Completing the Privacy Breach Report Form

The headings below correspond to the sections of the Privacy Breach Report Form.

Information of Organization/Custodian/Public Body

- **Date of the report**

  The date of the report should be on or near the date the report is submitted to the Commissioner. The information in the report should be as accurate as possible as of the date of the report.[3]

- **Name of Organization/Custodian/Public Body**

  Provide the legal name of the organization, custodian or public body.

  PIPA: the organization is the organization with control of the personal information that is involved in the breach (section 34.1).

  HIA: the custodian is the custodian with custody or control of the individually identifying health information that is involved in the breach (section 60.1(2)).

  Refer to page 3 for a brief discussion of custody vs. control.

- **Address of Organization/Custodian/Public Body**

  Provide the address of the organization, custodian or public body.

- **Organization/Custodian/Public Body file number** (if applicable)

  Include any file number that the organization, custodian or public body has assigned to the breach, so that it can be referenced by the Commissioner's office when communicating with the organization, custodian or public body.

- **Contact information for a person who can answer the Commissioner's questions about the breach**

  Provide the name, title/position and contact information for the person who, on behalf of the organization, custodian or public body, can answer the Commissioner's questions about the breach (PIPA Regulation, section 19(h); *Health Information Regulation*, section 8.2(2)(l)). This is the person the OIPC will communicate with about the breach.

[3] Under PIPA, the Commissioner will make the decision whether notification to individuals is required based on the information before the Commissioner at the time of the decision.

- **PIPA non-profit organizations**

  This section applies only to those not-for-profit organizations that meet the definition of a "non-profit organization" in section 56(1)(b) of PIPA.

  For purposes of PIPA, a non-profit organization is an organization that is:

  - Incorporated under the *Societies Act* or the *Agricultural Societies Act*, or
  - Registered under Part 9 of the *Companies Act*

  These non-profit organizations must notify the Commissioner of a reportable privacy breach when the personal information involved in the breach was collected, used or disclosed by the organization **in connection with a commercial activity** carried out by the organization.

  Section 56(1)(a) of the Act defines what is a commercial activity.

  A privacy breach involving the personal information of employees of a non-profit organization (as defined in section 56) can be subject to the mandatory breach notification requirements in PIPA. The OIPC has determined that employees hired to perform functions necessary to carry out a commercial activity are hired "in connection with" that commercial activity (Order P2017-07). The Commissioner has required non-profit organizations to notify employees whose personal information was the subject of a breach. For example, in breach decision P2018-ND-003, the individuals affected by the breach worked as a housekeeper, cook and kitchen staff, banquet server, or maintenance worker. These are functions that are necessary to carry out the non-profit organization's commercial activity of operating a recreational facility.

  When a not-for-profit organization does not meet the section 56 definition of a non-profit organization (i.e. it is established in some way other than by the Acts named in section 56(1)(b), such as by private Act, under federal or other provincial legislation or as an unincorporated association) PIPA applies fully to the organization and the organization must report a breach to the Commissioner in accordance with section 34.1 of PIPA, whether or not the organization is carrying on a commercial activity.

- **Third party reporting the breach** (if applicable)

  Occasionally, the entity reporting the breach to the Commissioner is not the organization or custodian that is required to report the breach to the Commissioner.

  Complete this section of the form if the entity reporting the breach is **not** the organization, custodian or public body responsible for reporting the breach to the Commissioner (i.e. the organization, custodian or public body named at the beginning of the form). Indicate the relationship with the organization, custodian or public body, whether the breach has been reported to the organization, custodian or public body, and whether the reporting entity is authorized to report the breach to the Commissioner on behalf of the organization, custodian or public body.

Note: Under HIA, an affiliate of a custodian must as soon as practicable notify the custodian (in accordance with the regulations) of any privacy breach of individually identifying health information in the custody or control of the custodian (section 60.1(1)). For the requirements of that notice to the custodian, see the *Health Information Regulation* (section 8.2(1)).

Breach Description

- **Date breach occurred and date breach ended**

  Provide the date on which the breach started and ended. If the actual date(s) of the breach are not known at this time, provide the suspected date range during which the breach occurred (PIPA Regulation, section 19(b); *Health Information Regulation*, section 8.2(2)(c)).

- **Date breach was discovered**

  Provide the date on which the breach was discovered (*Health Information Regulation*, section 8.2(2)(d)).

- **Total number of individuals affected**

  Provide the number (or an estimate if the actual number is not yet known) of the individuals whose personal information or individually identifying health information is involved in the breach (PIPA Regulation, section 19(e); *Health Information Regulation*, section 8.2(2)(g)).

- **Was the information collected in Alberta?**

  Indicate if any of the personal information or individually identifying health information involved in the breach was collected in Alberta.

  If yes, provide the number of individuals (or an estimate if the actual number is not yet known) of the individuals whose information was collected in Alberta.

- **Type of breach involved**

  Indicate the type of breach involved:

  - A loss of personal information or individually identifying health information (e.g. theft of information from an office, home or vehicle; organization does not know where the information is; information lost during office relocation)
  - Unauthorized access to personal information or individually identifying health information (e.g. electronic system compromise; ransom demand; phishing or social engineering; payment card skimming; break-in without theft; employee accessing information without authorization)

- Unauthorized disclosure of personal information or individually identifying health information (e.g. transmission errors by email, fax, mail or verbally; information improperly shared on internal network drives, social media, etc.)

- **Location of the breach**

  Provide the address of the physical location where the breach occurred.

- **Describe the circumstances of the breach and the causes**

  Provide a description of the breach and the causes of the breach, if known (PIPA Regulation, section 19(a); *Health Information Regulation*, section 8.2(2)(b)). ***Do not include personal information or identifying health information about the individuals whose information is involved in the breach ("individually identifying information").***

- **Describe how the breach was discovered and who discovered it**

  Provide a description of how the breach was discovered, and the circumstances associated with the discovery.

  Also indicate the person who discovered the breach, including their name and their title or position within the organization, custodian or public body.

  If the person who discovered the breach is a service provider to the organization, custodian or public body, provide the name of their employer and indicate the relationship between their employer and the organization, custodian or public body.

  If there has been a delay between the discovery of the breach and reporting it to the Commissioner, provide an explanation for the delay:

  - PIPA requires organizations to notify the Commissioner without unreasonable delay (section 34.1)
  - HIA requires custodians to notify the Commissioner as soon as practicable (section 60.1(2))

Notice to Affected Individuals

- **Have affected individuals been notified?**

  Indicate if the individuals affected by the breach have been notified.

  Provide the information that has been given or will be given to the affected individuals. Where possible, attach a copy of the actual notice being given to the individuals. If notice was or is to be given by telephone, attach a copy of the script used (HIA requires that notice to affected individuals be in writing). ***Do not include individually identifying information.***

Describe the form in which the notice was given (e.g. by letter, email) and the date on which or date range during which notification was given.

PIPA

The Commissioner has the power to require an organization to notify affected individuals when a privacy breach presents a real risk of significant harm as a result of the breach (section 37.1). This does not prohibit or restrict an organization from notifying individuals on their own initiative (section 37.1(7)). Although the Commissioner has an expedited process for reviewing breach reports, the Commissioner encourages organizations to not wait for direction from the Commissioner but to immediately notify affected individuals on their own initiative when the organization believes that there exists a real risk of significant harm to the individuals as a result of the breach.

Organizations must provide the Commissioner with a description of any steps the organization has taken to notify affected individuals of the privacy breach (PIPA Regulation, section 19(g)).

The criteria for what is to be included in a notice to an affected individual are set out in section 19.1 of the PIPA Regulation. Notice must be given to the individual directly unless the Commissioner determines that direct notification would be unreasonable in the circumstances (PIPA Regulation, section 19.1(2)).

HIA

HIA places the responsibility on custodians for determining whether to notify individuals about a breach. Custodians are required to notify individuals[4] where there is a risk of harm to the individuals as a result of a breach of individually identifying health information.

A custodian's notification to the Commissioner of a privacy breach must include a non-identifying copy of the information that has been or will be provided in the notice to affected individuals together with a statement indicating the method referred to in section 103 of HIA that has been or will be used to give notice to the individual (*Health Information Regulation*, section 8.2(2)(j)).

The notice to an affected individual must be in writing and include the information set out in section 8.2(4) of the *Health Information Regulation*.

[4] A custodian may decide not to notify an affected individual if notification could reasonably be expected to result in a risk of harm to the individual's mental or physical health. In such cases, the custodian must immediately notify the Commissioner of the decision not to notify the individual (HIA, section 60.1(5)). See Appendix A.

Personal or Health Information Involved

- **List the types of personal information or health information involved**

  Specify the various elements of personal or health information involved in the breach (PIPA Regulation, section 19(c); *Health Information Regulation*, section 8.2(2)(e)). ***Do not include individually identifying information.***

  Examples of personal information or health information include but are not limited to:

  - Name
  - Address
  - Email address
  - Telephone number
  - Social Insurance Number (SIN)
  - Driver's licence number
  - Education history
  - Employee number, pay, benefits, disciplinary records, performance evaluations
  - Credit card information
  - Banking and other financial information
  - Personal Health Number
  - Medical diagnostic, treatment and care information
  - Registration information as defined in HIA

Harm

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

  Identifying the harm(s) that could result from the breach is a component in the overall assessment of the risk to an individual as a result of the breach.

  Harm means some damage or detriment or injury that could be caused to affected individuals as a result of the incident. Some examples of harm that could flow from a breach of personal information or individually identifying health information are:

  - A breach of an individual's name and credit card number could result in identity theft and financial fraud.

- A breach of an individual's name, driver's licence and SIN could result in identity theft and fraud.
- A breach of an individual's diagnostic, treatment and care information could result in hurt or humiliation.
- A breach of name and subscription to an adult magazine or website could result in reputational harm.
- A breach of an individual's disciplinary letter could result in humiliation.

PIPA

The test for reporting a beach is "a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure" (section 34.1). The damage or detriment or injury that could be caused to affected individuals as a result of the incident must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

Examples of significant harm include:

- Bodily harm
- Embarrassment, hurt or humiliation
- Damage to reputation or relationships
- Loss of employment, business or professional opportunities
- Financial loss
- Identity theft
- Fraud
- Negative effects on a credit record
- Damage to or loss of property
- Blackmail or extortion
- Email phishing or spear-phishing attacks

HIA

The test for reporting a breach is "risk of harm to an individual as a result of the loss or unauthorized access or disclosure" (section 60.1(2)). A custodian must consider all relevant factors, including the factors set out in section 8.1(1) of the *Health Information Regulation* (HIA, section 60.1(3)).

Provide a description of the type(s) of harm to an individual as a result of the breach (*Health Information Regulation*, section 8.2(2)(f)). Some of the harms contemplated by the legislation include:

- Identity theft
- Fraud
- Embarrassment

- Mental harm
- Physical harm
- Financial harm
- Damage to reputation
- Adversely affect the provision of a health service

Risk Assessment

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

PIPA

Provide an assessment of the likelihood that there is a **real risk of significant harm** to an individual as a result of the breach (PIPA Regulation, section 19(d)). The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the breach and the possible harm.

To determine whether a there is a real risk of significant harm to an individual, the organization must consider all the circumstances surrounding the breach. Factors that influence the likelihood of significant harm resulting from the breach include but are not limited to:

- What is the nature of the information involved?
- Who obtained or could have obtained access to the information?
- How many persons was the information exposed to?
- Is there any personal or professional relationship between the affected individual and the unauthorized recipient of the information?
- Were there security measures in place to prevent unauthorized access, such as encryption?
- How long was the information exposed?
- Is there evidence of malicious intent or purpose, such as theft, hacking or malware?
- Could the information be used for criminal purposes, such as for identity theft or fraud?
- Was the information recovered?
- How many individuals are affected by the breach?
- Are there vulnerable individuals involved, such as youth or seniors?

Examples of what is considered a real risk of significant harm can be found in the Commissioner's breach notification decisions at www.oipc.ab.ca.

HIA

Provide an explanation of how the **risk of harm** to an individual as a result of the breach was assessed (*Health Information Regulation*, section 8.2(2)(f)). Include a description of the custodian's consideration of all relevant factors including the following factors set out in section 8.1(1) of the *Health Information Regulation*:

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

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

(c) whether there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud;

(d) whether there is a reasonable basis to believe that the information is of a type that could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual who is the subject of the information;

(e) whether there is a reasonable basis to believe that the loss of or unauthorized access to or disclosure of the information has adversely affected or will adversely affect the provision of a health service to the individual who is the subject of the information;

(f) in the case of electronic information, whether the custodian 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;

(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;

(h) in the case of a loss of information that is subsequently recovered by the custodian, whether the custodian can demonstrate that the information was not accessed before it was recovered;

(i) in the case of an unauthorized access to or disclosure of information, whether the custodian is able to demonstrate that the only person who accessed the information or to whom the information was disclosed

  (i) is a custodian or an affiliate,

  (ii) is subject to confidentiality policies and procedures that meet the requirements of section 60 of the Act,

(iii) accessed the information in a manner that is in accordance with the person's duties as a custodian or affiliate and not for an improper purpose, and

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

If the custodian is able to demonstrate that a circumstance set out in (f) to (i) above applies in the case of the breach, the custodian is not required to give notice of the breach to the Commissioner under section 60.1(2) of HIA (*Health Information Regulation*, section 8.1(2)).

Risk Mitigation

- **Describe the steps taken to reduce the risk of harm to affected individuals**

  List the actions taken by the organization, custodian or public body to reduce the risk of harm to affected individuals as a result of the breach (e.g., information recovered; undertaking by unauthorized recipient that the information was not viewed, used, or disclosed and was securely destroyed; device remotely disabled or wiped permanently; credit report monitoring). Include any actions that are planned but not yet implemented (PIPA Regulation, section 19(f); *Health Information Regulation*, section 8.2(2)(h)).

- **Describe the steps taken to reduce the risk of a similar event occurring in the future**

  List the actions taken by the organization, custodian or public body to reduce the risk of similar breach occurring in the future (e.g., mobile devices encrypted; physical locks changed; policies and procedures revised; training implemented; known risks monitored; auditing processes implemented). Include any actions that are planned but not yet implemented.

  This is a requirement for custodians under section 8.2(2)(i) of the *Health Information Regulation*.

Additional Information

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

  A privacy officer is the person responsible for privacy within an organization, custodian or public body. The privacy officer should be notified of a breach in order to assist in managing the breach, implementing breach protocols, and notifying the Commissioner and individuals. Some organizations, custodians and public bodies may not have a designated privacy officer.

  Indicate if the privacy officer or person responsible for security has been informed of the breach and provide their contact information.

- **Have the police or any other authorities or organizations been notified about the incident?**

  Indicate if other entities have been notified of the breach and provide their contact information.

  An organization, custodian or public body may notify other entities of the breach for different reasons. For example:

  - Police: if theft or other crime is suspected
  - Insurers or others: if required by contractual obligations
  - Professional or other regulatory bodies
  - Credit card companies and/or credit reporting agencies: it may be necessary to work with these companies to notify individuals and mitigate the effects of fraud
  - Other privacy commissioners: the breach may involve personal information or health information in several jurisdictions

- **Provide any additional relevant information regarding the privacy breach**

  Add any other information that the organization, custodian or public body considers relevant (*Health Information Regulation*, section 8.2(2)(m)).

Submitting to the Commissioner

Organizations are required to notify the Commissioner of a reportable breach under PIPA **without unreasonable delay**.

Custodians are required to notify the Commissioner of a reportable breach under HIA **as soon as practicable**.

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

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

Office of the Information and Privacy Commissioner of Alberta
410, 9925 - 109 Street
Edmonton, AB T5K 2J8
Fax: (780) 422-5682

For general information about responding to a privacy breach, please contact the OIPC by telephone at (780) 422-6860 or toll free at 1-888-878-4044. Information provided does not constitute legal advice, is not binding on the Commissioner, and does not mean an organization or custodian has fulfilled its legal obligation to report a privacy breach to the Commissioner.

Appendix A: For Health Custodians Only - Notice to Commissioner of Decision Not to Give Notice of Breach to Individual(s)

A custodian may decide not to notify one or more affected individuals of a privacy breach if notification could reasonably be expected to result in a risk of harm to the individual's mental or physical health. In such cases, the custodian must immediately notify the Commissioner of the decision not to give notice of the privacy breach to the individual (HIA, section 60.1(5)).

Complete **Appendix A of the Privacy Breach Report Form** to notify the Commissioner of the decision to not notify an individual of the breach. A copy of the Privacy Breach Report Form must also be attached (*Health Information Regulation*, section 8.3)

Appendix B: For Health Custodians Only - Request for Authorization to Give Notice of Breach by Substitutional Service

A custodian may give notice of a reportable breach to an affected individual by substitutional service if so authorized by the Commissioner (HIA, section 103(c)).

Complete **Appendix B of the Privacy Breach Report Form** to request the Commissioner for authorization to provide notice by substitutional service. Include a statement of the reasons for the request (*Health Information Regulation*, section 8.2(2)(k)).

Please attach a copy of the Privacy Breach Report Form.