PHIA Guidelines

Custodian Responding to a Privacy Complaint

These are guidelines to assist you in understanding the privacy complaint process under the **Personal Health Information Act** (PHIA). You can find additional resources on our website.

Privacy Complaints

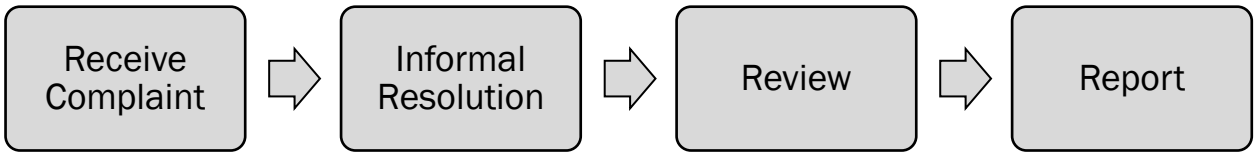
A person may make a privacy complaint to the Office of the Information and Privacy Commissioner (OIPC) if they believe, on reasonable grounds, that a custodian (a person or organization who holds personal health information) has contravened or is about to contravene PHIA in respect of personal health information. Such contravention includes improper collection, use, or disclosure of personal health information or a privacy breach.

Remedies

Following an investigation of a privacy complaint, the Commissioner may recommend that a custodian stop collecting, using, or disclosing personal health information or destroy personal health information in its custody. The Commissioner may also make recommendations related to a custodian's information practices, policies, or procedures.

The Complaint Process

1. OIPC receives a complaint. We will provide the complaint to the custodian and you will have 14 days to respond. The complainant also has 14 days to make any submissions or arguments in support of their complaint.
2. OIPC will generally work with you and the complainant to try to reach an informal resolution of the complaint.
3. If we have not resolved the complaint, OIPC may conduct a review of any unresolved issues.
4. If necessary, OIPC will issue a Commissioner's report with recommendations for the custodian.



We explain the steps in this process in more detail below.

Receiving a Complaint and Making Submissions

After our Office receives a complaint, we will assign it to an Access and Privacy Analyst (Analyst). The Analyst will contact you to notify you of the complaint. The Analyst will ask you to provide documents and written representations (submissions) relevant to the complaint.

Your response to our Office is due within 14 days from that date. This response must include the following:

- a response to the issues that the complainant raised;
- any correspondence or records related to the complaint or that might assist in clarifying or resolving the complaint;
- any policies or procedures you have that relate to the collection, use, or disclosure of the personal health information at issue in the complaint;
- any remediation plan you have developed to deal with breaches of privacy or personal health information; and
- any additional information you wish to provide in relation to the complaint.

You should provide these documents as clearly labelled, separate files.

If you do not provide your submissions within 14 days, we will proceed with the investigation based on the relevant information available to OIPC. Without your written submissions, it is unlikely that we will be able to resolve the matter informally, and we will likely have to move the matter to a review and issue a Commissioner's report. If you are unable to provide written submissions, you should contact OIPC to explain why and to discuss acceptable alternatives.

Claims of Unauthorized Collection, Use, or Disclosure

If the complaint involves a claim that the custodian had no authorization to collect, use, or disclose personal health information, the custodian's submissions should reference the sections of PHIA it relies on for such collection, use, or disclosure of personal health information with reference to the relevant provisions of the Act.

Claims of a Privacy Breach

If the complaint involves a privacy breach, the custodian should explain the steps it took in managing the breach, including steps it took to:

- investigate the breach;
- contain the breach;
- evaluate the risks to affected individuals;
- notify affected individuals; and
- prevent future breaches.

The custodian should also explain what safeguards it had in place to protect the personal health information at the time of the privacy breach and whether it plans to make changes to its safeguards in response to the privacy breach. Safeguards relevant to a privacy breach may include:

- administrative safeguards (information practices, policies, procedures, employee training, etc.);

- physical safeguards (locked cabinets, alarm systems, secure storage, etc.); and
- technical safeguards (firewalls, data encryption, multi-factor authentication, etc.).

Informal Resolution

The Analyst will usually focus on resolving the matter informally within a reasonable period of time.

During informal resolution, the Analyst will use your submissions as well as the submissions we receive from the complainant to understand the nature of the complaint and attempt to identify possible opportunities to resolve the complaint in a way that satisfies both the complainant and the custodian. Generally, the Analyst will provide you and the complainant with an assessment after reviewing your submissions and the complainant's submissions.

During our efforts at informal resolution, it is important that you respond promptly to the Analyst's questions or requests. If you do not participate in this process we may proceed to a review without your input.

Possible informal resolution of a complaint may include:

- the custodian acknowledging a privacy breach and filing a breach report with our Office;
- the custodian taking steps to stop collecting, using, or disclosing certain personal health information;
- the custodian agreeing to review or make changes to its information practices, policies, or procedures; or
- other outcomes that are agreeable to the complainant and the custodian and compliant with PHIA.

In some cases, our initial assessment of a complaint may conclude that PHIA authorizes the custodian's collection, use, or disclosure of the complainant's personal health information and the complainant may choose to conclude their complaint on that basis.

Review

If there are any issues in the complaint that we have not resolved in the informal resolution period, then our Office may conduct a review and, if necessary, issue a report with the Commissioner's recommendations. If the Analyst believes more information is necessary, they will ask you to provide further submissions and give you a deadline. We might not consider submissions that we receive after that deadline.

The Commissioner may decide not to conduct a review in limited circumstances under section 67(3) of PHIA. Should the Commissioner make this decision, we will notify you of the reason.

Commissioner's Report

If necessary, our Office may write and release a report of our findings following an investigation of a privacy complaint. OIPC publishes Commissioner's reports on our website and we will send you a copy.

OIPC will consider your submissions and the complainant's submissions during the report process. We may quote your submissions in the Commissioner's report. If you have provided submissions or other information that you feel is confidential that you do not want us to quote, you should notify the Analyst. However, procedural fairness requires the Commissioner to provide reasons for any decisions and recommendations. Therefore, we may still need to explain your position on the matter in the report.

The Commissioner's report may contain recommendations that the custodian:

- stop collecting, using, or disclosing personal health information in contravention of PHIA;
- destroy personal health information collected in contravention of PHIA;
- implement, modify, or stop an information practice, policy, or procedure;
- not begin an information practice, policy, or procedure; or
- take other actions related to the privacy aspect of the complaint.

The Commissioner may decide not to make any recommendations. If there are no recommendations, the report will explain why.

After you receive the Commissioner's report with recommendations, the custodian has 15 days to decide whether to follow the Commissioner's recommendations. Regardless of the custodian's decision, the custodian must give written notice of its decision to the complainant and our Office.

If you have any questions or concerns about the complaint process, please do not hesitate to contact our Office at:

Office of the Information and Privacy Commissioner
PO Box 13004, Station A
St. John's, NL A1B 3V8
Phone: (709) 729-6309 Fax: (709) 729-6500
Toll Free: 1-877-729-6309
commissioner@oipc.nl.ca
https://www.oipc.nl.ca