



Guidelines for Responding to Patient and Employee Complaints

This section will:

- explain patients' and employees' rights regarding complaints related to their personal information
- identify the requirements of an effective complaint management process
- describe the ten steps of managing a complaint

Under the BC Personal Information Protection Act (PIPA), a practice must have a process to respond to complaints about its privacy practices or how personal information was handled. For example, individuals may have a complaint about the scope of records produced by the practice in response to a request for their personal information, collection practices, a disclosure of personal information without consent or a privacy breach. Having an accessible and effective complaint management process is an important aspect of managing privacy risks and helps to promote accountability, openness and trust. It also allows a practice to address complaints in a timely manner, identify systemic or ongoing compliance issues and demonstrate a commitment to privacy.

In a complaint involving a privacy breach, responding in an effective and timely manner is critical. For guidance on responding to privacy breaches see [Guidelines for Responding to a Privacy Breach](#) or [Privacy Breaches: Tools and Resources](#).

Best practices for setting up a complaint management process include the following steps:

- Decide who in the practice will be responsible for receiving, responding to and managing complaints about the practice's compliance with PIPA (this could be the designated Privacy Officer or it could be delegated to another individual).
- Develop and document a complaint procedure that is confidential, accessible, simple and easy to use.
- Develop a complaint form to assist in recording the complaint and collecting the necessary information required to investigate and respond.
- Document the process and ensure all employees are aware of the complaint management process so they can direct a complainant to the appropriate person for follow-up or, in the absence of this individual, provide information to the complainant on how they may proceed with a complaint.
- Ensure the process includes providing reasons for a decision in sufficient detail to suit the nature of the complaint.



- Reinforce that addressing a complaint quickly helps maintain or even increase the patient's trust in the practice.

Steps for Managing a Complaint

When the complaint is received in writing, record the date of the complaint and acknowledge its receipt.

- If the complaint is received verbally, record the nature of the complaint and the details.
- If necessary, contact the individual to clarify the complaint.
- Ensure that the complaint process is fair, impartial, and confidential.
- Investigate the complaint by gathering information and fully understanding the circumstances. Clarify specifics of the complaint by asking questions such as:
 - What events led to the complaint?
 - What personal information is involved and what happened to it?
 - When and where did the event(s) occur?
 - Who was involved (e.g., employees, locum physicians, visiting specialists, physicians-in-training, third party contractual employees)?
- Where a complaint is justified, determine the specific cause and
 - take measures to remedy the situation
 - communicate this to relevant employees involved
 - record all decisions and actions taken to prevent recurrence
- If a complaint cannot be substantiated, document the investigation so it can be explained to the complainant.
- Notify the complainant of the outcome and the reasons for the decision regardless of whether the complaint can be substantiated or not. Where applicable, inform him or her of the steps taken to rectify the concerns.
- Inform the complainant of the right to appeal to the Information and Privacy Commissioner, if they are not satisfied with the practice's response to the complaint, within 30 business days starting from the date the physician's office communicated to the complainant its reasons for the response.
- If applicable, prevent recurrence through techniques such as modifying or updating policies and procedures, providing employee training and implementing improved privacy and security safeguards.