COLLEGE OF PHYSICIANS
& SURGEONS OF ALBERTA

Privacy Directive
Access to personal information

1. PURPOSE

In order to meet the requirements and obligations when managing personal information, this Privacy Directive details the process for individuals to access information CPSA holds about them.

2. DEFINITIONS

Definitions of terms used in this directive are located in section 2 of the *Privacy and Confidential Information Policy*.

3. GENERAL REQUIREMENTS

a. At any time, subject to limited exceptions as described in section 6, an individual may access the information CPSA holds, uses, and discloses about them.

b. To safeguard personal information, individuals requesting access to personal information may be required to provide identification to confirm identity and authorize access.

c. CPSA will promptly correct or complete any personal information in its custody and control found to be inaccurate or incomplete. CPSA will note all unresolved differences that pertain to accuracy or completeness in the individual's file. Where appropriate, CPSA will circulate amended information to third parties to whom it had previously disclosed the information.

d. CPSA handles all requests for access to information in accordance with CPSA's privacy how-to sheets:

    i. *Responding to Access Requests-HPA,* the process for CPSA departments to respond to requests for copies of documents from their files; and

    ii. *Responding to Access Requests-PIPA*, the process for the Privacy Team to respond to access requests for personal information under PIPA. Direct all requests for personal information to the Privacy Team.

e. Documents created by the Hearing Tribunal, a quasi-judicial body, fall under FOIP. Requests for Hearing Tribunal documents must be responded to in compliance with FOIP.

4. REQUESTING ACCESS TO PERSONAL INFORMATION

Requests must be in writing and should include:

a. sufficient detail as to what personal information is being requested for review, and

b. whether the individual wants a copy of his or her record, or to examine the record.

5. RESPONDING TO ACCESS REQUESTS

a. CPSA must provide a written response to the individual within 45 days of receiving the written request, and must either announce approval and access procedures, or provide an explanation as to why they are denied or have limited access.

b. If the request is not clear, CPSA should seek clarification of the request before beginning to review records. Waiting for the clarification suspends the 45-day response period.

c. CPSA must review the requested record(s) prior to responding to a request to determine if the record(s) contain any information that cannot be shared. There are strict rules as to what information cannot be shared, as identified in section 6 of this directive, so seek advice from the Privacy Team.

d. The response should contain the following information:
   - decision and explanation of entitlement to view personal information,
   - when access will be given,
   - a fee estimate if applicable,
   - if a copy was requested, the copy may be included at this time or notice given that it will follow within a specified time period,
   - if access to all or part has been refused, the reason for refusal including the provisions of *PIPA* or the *HPA* that substantiate the refusal, and
   - recourse for appeal including the Privacy Officer's contact information and an explanation of the appeal process under section 46 of *PIPA*.

e. If there is a need for the access response to exceed 45 days, CPSA must send a letter to the individual, within the initial 45-day period, explaining the delay. Common justified delays would include:
   - waiting for advice from legal counsel or the OIPC, or
   - considering an unusually complex or large request.

   PIPA, section 31, provides further detail on justified delays.

f. Upon request and within the required time period of 45 days, CPSA must provide an account of the use and disclosure of personal information. In providing an account of disclosure, when it is not possible to provide an actual list, CPSA must provide a list of organizations to which it may have disclosed personal information.

6. REVIEWING RECORDS

a. In certain situations, CPSA may not be able to provide access to all the personal information that it holds about an individual; prior to granting access to personal information, CPSA's Privacy Team must review the record to determine whether the information can/should be released.

b. If CPSA cannot provide access to personal information, it must provide the reasons for denying access upon request.

c. CPSA **must** provide the following information to individuals upon their request.

- personal information contained in records under the custody or control of CPSA subject to the limited exceptions described in 6d and 6e below,
- the purposes for which personal information is being/has been used, and
- the names of the third parties that CPSA has disclosed to, and/or will continue to disclose to and for what purpose.

d. CPSA **may** refuse access, even if requested, if the information:

- is protected by legal privilege, or
- would reveal confidential commercial information that would not be unreasonable to withhold, or
- is collected in relation to an investigation into the professional conduct of the individual or a legal proceeding, or
- if disclosed, might result in that type of information no longer being provided even though it would be reasonable for it to be provided, or
- is collected by a mediator or arbitrator or created during a mediation or arbitration, or
- is related to, or that may be used in, the exercise of prosecutorial discretion.

e. CPSA **must not** provide access to individuals if the information:

- could reasonably be expected to threaten the life or security of another individual, or
- would identify or otherwise reveal personal information about another individual.

- If an individual is requesting information that may reveal the personal information of another individual, then CPSA's Privacy Team is obliged to investigate the reasonability of severing that information from the record or a copy of the record in order to accommodate the original request to the greatest extent.

7. COMPLIANCE

Team member, with the exception of council/committee members, or vendor failure to comply with this policy is cause for disciplinary action up to and including termination of employment or business relationship and, where applicable, legal or other action. Council/Committee members' failure to comply with this policy is addressed by the council president.

If you have a questions or concerns about CPSA's handling of confidential information, please contact CPSA's Privacy Team.

8. REFERENCES

This directive falls under the *Privacy and Confidential Information Policy*.

Related Policies

- *Internet Access & Use*
- *Software Standards*
- *Records and Information Management*
- *File Retention*

Privacy Directives

- *Acceptable Uses of Networks and Electronic Devices*
- *Access to Personal Information*
- *Privacy and Information Management Training*
- *Protecting Confidential Information*
- *Protecting Information when Contracting for Services*
- *Team Member Arrival/Departure*

Privacy How-to Sheets

- *Locking & Securing Computers*
- *Printing Private & Confidential Documents*
- *Privacy Breach Response*
- *Recording Audio or Videoconferences*
- *Redacting Information from Documents*
- *Responding to Access Requests-HPA*
- *Responding to Access Requests-PIPA*
- *Sharing Confidential Information Electronically*