cpsa

COLLEGE OF PHYSICIANS
& SURGEONS OF ALBERTA

Privacy & Confidential Information Policy

Contents

cpsa
COLLEGE OF PHYSICIANS & SURGEONS OF ALBERTA

1. PURPOSE

The College of Physicians & Surgeons of Alberta (CPSA) is responsible for maintaining and protecting the confidential information under its control. This policy:

a. Documents practices as related to confidential information
b. Provides guidance to staff as they address challenges associated with handling confidential information
c. Aims to achieve statutory and regulatory compliance

2. DEFINITIONS

Business contact information:	An individual's name, position name or title, business telephone number, business address, business e-mail, business fax number and other similar business information used to contact an individual in his or her capacity as an employee of an organization.
CPSA:	The College of Physicians & Surgeons of Alberta as established in section 1 of Schedule 21 of the *Health Professions Act*.
Confidential information:	Not limited to, but includes: i. all personal information as defined by the *Personal Information Protection Act;* ii. all health information as defined by Alberta's *Health Information Act* to which CPSA may have access; iii. all protected employee information; and iv. iv. all business information deemed to be confidential.
Employee:	An individual employed by CPSA, and from whom CPSA collects personal information, including a volunteer, council member, committee member, contractor and an agency placement who from time to time performs a service on behalf of CPSA.
HIA:	*Health Information Act,* H-5, RSA 2000 and applicable regulations.
HPA:	*Health Professions Act,* H-7, RSA 2000 and applicable regulations.
Leadership Team:	The Registrar, Assistant Registrars, Chiefs, and Directors of CPSA.
OIPC:	Alberta's Office of the Information and Privacy Commissioner.
Personal information:	Information about an identifiable individual excluding business contact information.
PIPA:	*Personal Information Protection Act*, S.A. 2003 c. P 6.5 and applicable regulations.

Policy/policies:	Privacy and information-related policy instruments of CPSA including this policy and all directives or procedures falling under it.
Potential employee:	An individual who has an open application for employment with CPSA.
Privacy Team:	The Privacy Officer and Privacy Coordinator. The Privacy Officer delegates responsibilities for administration of CPSA Privacy Management Program to the Privacy Coordinator.
Vendor:	An individual or organization that performs a service on behalf of CPSA, pursuant to an agreement with CPSA; of particular relevance are vendors providing services that involve access to CPSA information or that are otherwise information-related, but from whom no personal information would be collected.

3. POLICY STATEMENT

As a professional regulatory body under the HPA, CPSA has a responsibility to take all reasonable measures to safeguard confidential information in its custody and control or to which it has access.

Technical environments and best practices related to information handling change quickly and often. In response to this reality, CPSA has delegated responsibility for confidential information to its Privacy Officer and senior technical staff.

4. CLASSIFICATION OF INFORMATION

CPSA staff must treat, minimally handle and protect all information deemed confidential as described in this policy. This policy and all directives falling under it are the minimum standards CPSA must use. Confidential information of a particularly sensitive nature may be so classified. The Leadership Team may impose further limitations upon the collection, use, storage, retention and/or disclosure of such information.

5. ACCOUNTABILITY

CPSA is responsible for maintaining and protecting the confidential information under its control.

a. Accountability for ensuring privacy compliance rests with the Leadership Team of CPSA. The Registrar will designate one employee as Privacy Officer responsible for CPSA's compliance with privacy legislation. The Privacy Officer may delegate other individuals within CPSA, such as the Privacy Coordinator, to act on their behalf or take responsibility for routine handling of confidential information.

b. CPSA shall implement policies and procedures to:
   - ☐ protect confidential information;
   - ☐ oversee compliance with privacy legislation;

☐ receive and respond to privacy inquiries and complaints; and
☐ inform employees and vendors about these policies and procedures.

c. CPSA must provide all new employees with a policy orientation detailing organizational policies and obligations when accessing and/or handling confidential information.

d. CPSA is responsible for confidential information in its possession or control and ensuring that employees and vendors comply with CPSA's policies and procedures pursuant to relevant legislation and/or agreements.

e. CPSA will share its privacy policies and procedures to individuals upon request.

f. CPSA will comply with the provisions of any agreements governing access to and handling of information (including health information) and will comply with the HIA as required.

6. NOTICE (IDENTIFYING PURPOSES)

CPSA will identify the purpose for which it is collecting personal information either before or at the time of collection.

a. CPSA will communicate verbally, electronically or in writing that the primary purpose of collecting, using and/or disclosing confidential information is to conduct business authorized under legislation. Upon request, persons collecting confidential information will explain these identified purposes or refer the individual to the Privacy Team for further explanation.

b. Unless required by law, CPSA will not use or disclose confidential information previously collected for any new purpose without first obtaining the consent of the individual and documenting the new purpose.

7. CONSENT

The knowledge and consent of an individual is required for the collection, use and/or disclosure of confidential information except when authorized, required or permitted by legislation.

a. As a regulatory authority, provisions 14(b), 17(b) and 20(b) of PIPA allow CPSA to collect, use and disclose personal information without consent if it is authorized or required to do so under legislation.
   i. For example, with respect to applicants to and registered members of CPSA, personal information is collected, used and disclosed to consider and approve registration, and maintain an annual certificate of registration as set out in the HPA, Part 2, section 28. As such, consent is not required for this purpose.

b. If the collection, use and/or disclosure of confidential information is not authorized or required under the law, then at the time of collection, and in a

manner that is easily understood, CPSA will use reasonable efforts to ensure that an individual is advised of the identified purposes for which confidential information will be collected, used and/or disclosed.

c. Generally speaking, if consent is required, CPSA will seek consent to collect, use and disclose confidential information at the time of collection. However, CPSA may seek consent to use and disclose confidential information after it has been collected but before it is used or disclosed for a new purpose. Consent may be expressed or implied.

d. At any time, an individual may revoke consent to collect, use and/or disclose their confidential information if the purpose for collection/use/disclosure is not a requirement under legislation, and if doing so does not change or frustrate a legal obligation. If an individual revokes consent, CPSA will cease to use and disclose the confidential information, except as permitted or required under PIPA, the HPA or other relevant legislation. Revoked consent may limit CPSA's ability to serve that individual.

8. COLLECTION OF CONFIDENTIAL INFORMATION

CPSA will collect confidential information by fair and lawful means and will limit its collection of confidential information to that which is reasonable for the purposes identified.

a. CPSA collects confidential information routinely from regulated members, applicants, employees, potential employees, and periodically from experts and Albertans.

b. From time to time, CPSA may receive confidential information from other sources. These parties must represent that they have the authority to disclose the information before CPSA will obtain it.

c. CPSA will adhere to the provisions of all information sharing agreements made with those who may provide confidential information to CPSA. CPSA will also adhere to any privacy legislation relevant to such information.

9. USE OF CONFIDENTIAL INFORMATION

CPSA can use confidential information only for the purpose identified at the time of collection.

a. Only authorized employees and/or vendors may access confidential information.

b. CPSA cannot use information collected for one purpose for other purposes without clear legislative authority or individual consent.

c. CPSA staff can only access files containing confidential information in accordance with CPSA's directive, *Protecting Confidential Information*.

d. All employees using confidential information should be able to explain why CPSA needs it, how it will use it, how it will protect it, and if/how it might share it.

10. STORAGE OF CONFIDENTIAL INFORMATION

CPSA will store all files containing confidential information in accordance with CPSA's directive, *Protecting Confidential Information*.

11. DISCLOSURE OF CONFIDENTIAL INFORMATION

CPSA will not disclose confidential information for purposes other than those for which it was collected unless it has an individual's consent, or is authorized or required by legislation.

a. Confidential information **will** generally be disclosed:
   - ☐ to the individual about whom the information relates;
   - ☐ with the consent of the subject individual;
   - ☐ when clearly identified as information CPSA will disclose at the time of collection;
   - ☐ when deemed publically available information; or
   - ☐ as authorized or required by law.

b. Confidential information **will not** be disclosed:
   - ☐ when prohibited by law; or
   - ☐ when such disclosure would contravene the terms of an information sharing or other such agreement.

12. ACCURACY OF CONFIDENTIAL INFORMATION

CPSA will ensure confidential information is as accurate, complete and as current as possible.

a. Confidential information used by CPSA will be as accurate and complete as is reasonably possible.

b. CPSA will update confidential information about an individual upon notification from the individual.

c. CPSA will, whenever authorized and reasonable, allow individuals to update their own confidential information.

13. RETENTION OF CONFIDENTIAL INFORMATION

In accordance with PIPA section 35, CPSA will retain personal information only for as long as reasonably needed for business or legal reasons.

a. CPSA will maintain records of investigations and hearings, copies of ratified settlements and admissions of unprofessional conduct, and records of complete

registration applications and reviews for a minimum of ten years.

b. CPSA will maintain financial records for a minimum of six years following the year in which the record was made (e.g., all records pertaining to fiscal year 2012 must be maintained until fiscal year 2019).

c. CPSA Leadership Team will determine the retention schedules for other records containing confidential information.

14. PROTECTION OF CONFIDENTIAL INFORMATION

CPSA will take all reasonable measures to prevent unauthorized collection, use, disclosure, modification or access to confidential information.

a. All employees and vendors will protect all confidential information held by CPSA and respect the privacy of the individuals who are the subjects of that information.

b. All employees and vendors are required to sign a confidentiality and non-disclosure agreement, and to uphold all policies and procedures respecting privacy and security of confidential information. The agreement remains in effect even after termination of any business, contractual or employment relationship with CPSA.

c. CPSA will safeguard all confidential information in accordance with CPSA's directive, *Protecting Confidential Information*.

15. INDIVIDUALS' ACCESS TO PERSONAL INFORMATION

Upon request, CPSA will inform an individual of the existence, use and disclosure of their personal information and will give them access to that information. An individual may challenge the accuracy and completeness of the information and have it amended as appropriate.

a. CPSA will handle all access requests in accordance with CPSA's directive, *Access to Personal Information* and the Privacy Department how-to sheet, *Understanding Access Requests*.

b. Individuals and employees can seek access to their confidential information by contacting the Privacy Team at CPSA.

16. CONTRACTING FOR SERVICES

CPSA may contract a third party vendor to provide services involving access to confidential information. The vendor may only collect, use and/or disclose confidential information in accordance with CPSA policy and in accordance with any contract and/or agreement established between the vendor and CPSA.

a. All vendor contracts or subsequent agreements must include provisions to protect confidential information in the custody and control of CPSA.

b. All contracts and/or vendor agreements must comply with CPSA's directive, *Protecting Information when Contracting for Services*.

17. INCIDENT RESPONSE

CPSA will respond to any incident, real or potential, involving confidential information under its control which could significantly impact CPSA operations.

a. Employees will report all security breaches or privacy compliance issues to CPSA's Privacy Team, and complete the *Privacy Breach Response Form*.

b. The Privacy Team will investigate the breach and evaluate the severity based on the degree of harm to the individuals involved, the sensitivity of the information, and the degree of malicious intent. Additional staff will be involved in the investigation as necessary to determine the cause of the breach and to implement any corrective or disciplinary actions required.

c. If the Privacy Team determines a real risk of significant harm to an individual(s) exists as a result of the breach, the Privacy Officer must report the breach to the OIPC or other investigative bodies, pursuant to section 34.1 of PIPA.

d. d. CPSA will share the results of the investigation to appropriate staff and take any corrective action.

e. The appropriate Leadership Team member will apply any applicable disciplinary action.

18. POLICY REVIEW

CPSA will review all privacy related policies periodically, minimally every three years, to ensure they reflect current practice, legislation and/or technology.

a. Periodically, at the discretion of the Privacy Officer and when CPSA is contemplating significant changes to programs and/or practices, CPSA will conduct a thorough risk assessment to determine the effectiveness of current policy and procedures, and to identify gaps.

b. The Privacy Officer will also conduct ongoing ad hoc assessments of privacy risk and revise or update CPSA's policies as needed.

19. COMPLIANCE

Employee, 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.

Employees can direct any questions or concerns about CPSA's handling of confidential information to CPSA's Privacy Team.

20. REFERENCES

This policy is the umbrella under which other policies, directives and guidance documents fall.

Related Policies

- *Internet Access & Use*
- *Protecting Confidential Information When Using Email*
- *Software Standards*

Privacy Directives

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

Privacy How-to Sheets

- How-to sheet: *Locking & Securing Computers*
- How-to sheet: *Printing Private & Confidential Documents*
- How-to sheet: *Privacy Breach Response*
- How-to sheet: *Sharing Confidential Information Electronically*
- How-to sheet: *Understanding Access Requests*
- IT How-to sheets: *Set-up Remote Access (work computer, PC home computer, Mac home computer)*