College of Physicians & Surgeons of Alberta

Our policy on

Privacy & Confidential Information

Contents

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 or the College:	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 the CPSA may have access; iii. all protected employee information; and iv. all business information deemed to be confidential.
Employee:	An individual employed by the CPSA including a volunteer, council member, committee member, contractor and an agency placement who from time to time performs a service on behalf of the CPSA.
HIA:	*Health Information Act,* H-5, RSA 2000 and applicable regulations.
HPA:	*Health Professions Act,* H-7, RSA 2000 and applicable regulations.
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 the CPSA include this policy and all directives or procedures falling under it.
Potential employee:	An individual who has an open application for employment with the CPSA.
Vendor:	An individual or organization that performs a service on behalf of the CPSA, pursuant to an agreement with the CPSA; of particular relevance are vendors providing services that involve access to the CPSA information or that are otherwise information-related.

3. Policy Statement

As a professional regulatory body under the HPA, the 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, the 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 the CPSA must use.

Confidential information of a particularly sensitive nature may be so classified. Management may impose further limitations upon the collection, use, storage, retention and/or disclosure of such information.

5. Accountability

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

a. Accountability for ensuring privacy compliance rests with the management team of the CPSA. The Registrar will designate one employee as privacy officer responsible for the CPSA's compliance with privacy legislation. The Privacy Officer may delegate other individuals within the College to act on his or her behalf or take responsibility for routine handling of confidential information.

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

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

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

f. The 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)

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

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

b. Unless required by law, the CPSA will not use or disclose confidential information that was 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 the 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 the 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 *Health Professions Act,* 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, the 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, the CPSA will seek consent to collect, use and disclose confidential information at the time of collection. However, the 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, the 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 the CPSA's ability to serve that individual.

8. Collection of Confidential Information

The 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. The CPSA collects confidential information routinely from members, applicants, employees, potential employees, and periodically from experts and the general public.

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

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

9. Use of Confidential Information

The 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. The 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 the CPSA's *Directive on Protecting Confidential Information*.

d. All employees using confidential information should be able to explain why the 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

The CPSA will store all files containing confidential information in accordance with the CPSA's *Directive on Protecting Confidential Information*.

11. Disclosure of Confidential Information

The 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, or
- with the consent of the subject individual, or
- when clearly identified as information the CPSA will disclose at the time of collection, or
- 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

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

a. Confidential information used by the CPSA will be as accurate and complete as is reasonably possible.
b. The CPSA will update confidential information about an individual upon notification from the individual.
c. The 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, the CPSA will retain personal information only for as long as reasonably needed for business or legal reasons.

a. The 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. The 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 management will determine the retention schedules for other records containing confidential information.

14. Protection of Confidential Information

The 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 the CPSA and respect the privacy of the individuals who are the subjects of that information.
b. All employees and vendors are required 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 the CPSA.
c. The CPSA will safeguard all confidential information in accordance with the CPSA's '*Directive on Protecting Confidential Information*'.

15. Individuals' Access to Personal Information

Upon request, the 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. The CPSA will handle all access requests in accordance with the CPSA's *Directive on Access to Personal Information* and the Privacy Department Procedure Manual: *Responding to Access Requests*.
b. Individuals and employees can seek access to their confidential information by contacting the privacy officer at the College.

16. Contracting for Services

The 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 College policy and in accordance with any contract and/or agreement established between the vendor and the College.

a. All vendor contracts or subsequent agreements must include provisions to protect confidential information in the custody and control of the CPSA.
b. All contracts and/or vendor agreements must comply with the CPSA's *Directive on Protecting Information when Contracting for Services*.

17. Incident Response

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

a. Employees will report all security breaches or privacy compliance issues to the CPSA's privacy officer.
b. The privacy officer 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. Depending on the nature and severity of the breach, the privacy officer will notify the OIPC or other investigative bodies that a breach has occurred.
d. The CPSA will share the results of the investigation to appropriate staff and take any corrective action.
e. The appropriate supervisory/managerial staff will apply any applicable disciplinary action.

18. Policy Review

The 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 the CPSA is contemplating significant changes to programs and/or practices, the 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 the CPSA's policies as needed.

19. Compliance

Employee 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.

Employees can direct any questions or concerns about the CPSA's handling of confidential information to the CPSA's privacy officer.

20. References

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