



Policy Privacy	Replaces former policy:
	<input type="checkbox"/> Title: <input checked="" type="checkbox"/> N/A
	Date Effective: 2025-10-01
	Last Update:
Contact: Privacy and FOI Office	

Policy Statement

The College protects the privacy of licensees, applicants, team members, committee and Board members, members of the public and any other individuals we interact with.

1. Policy Rationale and Purpose

This policy addresses the full range of privacy requirements in the *Freedom of Information and Protection of Privacy Act* (FOIPPA) at a high level and establishes roles and responsibilities in complying with them. It provides licensees, applicants, team members, Board and committee members, members of the public and any other individuals we interact with confidence in the College’s management of personal information.

2. Policy Scope

The policy applies to all team members, Board and committee members and to all of the personal information in the College’s custody or under its control, whether in electronic, paper or other form.

3. Indigenous Data Sovereignty

As part of its commitment to cultural safety and humility, the College recognizes the importance of honouring Indigenous perspectives on data governance and sovereignty, in accordance with the grandmother perspective and an approach centred on the importance of relationship.

Where the College collects, uses or discloses will use best efforts to respect and uphold Indigenous data sovereignty, including the First Nations principles of Ownership, Control, Access and Possession (OCAP®), while also meeting compliance requirements under FOIPPA.



4. Legal and Regulatory Authority

This policy is linked to the following legislation and regulatory documents:

- Health Professions Act RSBC 1996 c. 183 (HPA)
- Freedom of Information and Protection of Privacy Act RSBC 1996, c. 165 (FOIPPA)
- Declaration on the Rights of Indigenous Peoples Act SBC 2019 c. 44(DRIPA)
- CHCPBC Bylaws

5. Other Relevant Policies and Documents

This policy is linked to the following other relevant policies and documents:

- Privacy Breach Management Policy and Appendix
- BC Office of the Human Rights Commissioner (2020) Disaggregated demographic data collection BC: The grandmother perspective
- First Nations Principles of OCAP®
- Information Technology policies regarding the use of information systems and devices
- Records and Information Management Policy
- Records and Information Management Manual

6. Key Partnerships

None identified at this time.

7. Identifying Purposes

The College collects, uses and discloses personal information in accordance with British Columbia's *Freedom of Information and Protection of Privacy Act (FOIPPA)*, *Health Professions Act (HPA)* and other applicable laws, including the College's Bylaws.

The College may collect personal information to:

- meet the College's duty under the HPA to protect the public;
- assess and issue decisions regarding registration and permit applications (including, for example, initial registration, renewal and reinstatement);
- perform criminal record checks on team members, licensees, and applicants;
- administer and facilitate examinations;
- facilitate participation in a supervision program of the College;
- maintain the College's register as required by the HPA;
- administer the College's quality assurance program;
- administer the College's professional practice advisory program;
- investigate and dispose of complaints against licensees and health profession corporations (HPCs);
- comply with the procedures and requirements of the Health Professions Review Board and participate in proceedings before the Health Professions Review Board;



- contact licensees about the College's programs or activities, and to obtain feedback about them;
- obtain opinions and feedback from licensees, HPCs and members of the public on regulatory issues (such as on draft College Bylaw amendments);
- respond to general inquiries;
- administer human resources activities (such as recruitment, selection, and onboarding of team members and Board and committee members, performance management, benefits administration, and employee engagement);
- administer finance activities (such as dispensing salaries, processing credit and debit card payments and issuing expense payments);
- facilitate collaboration and knowledge sharing amongst the College, licensees, members of the public and other interested parties or organizations (such as through hosting events and maintaining a newsletter distribution list);
- operate, manage and protect the College's physical and electronic assets and systems;
- act as authorized or required by applicable law, including but not limited to the *HPA*, *FOIPPA* and the College Bylaws.

8. Duties and Responsibilities

Registrar/CEO and Executive Director, Legal Services

The Registrar/CEO is accountable for our compliance with *FOIPPA*. The Registrar/CEO has delegated executive oversight of the College's Privacy Management Program to the Executive Director, Legal Services.

The Executive Director, Legal Services works with the Lead, Privacy, and FOI to manage the operations of the Privacy Management Program.

Lead, Privacy, and FOI

The Lead of Privacy and FOI manages the day-to-day operations of the Privacy Management Program. The Lead of Privacy and FOI, in consultation with the Executive Director, Legal Services, is responsible for:

- developing privacy controls relating to collection, use and disclosure of personal information and assessing such controls on an ongoing basis;
- monitoring all aspects of privacy practices and compliance,
- managing and responding to all privacy breaches;
- responding to and managing all privacy complaints;
- managing the conduct of all privacy impact assessments (PIA);
- liaising with the Office of the Information and Privacy Commissioner of British Columbia, including in relation to investigations;
- creating, maintaining and coordinating delivery of privacy training to team members and Board and committee members;
- acting as an expert resource for the organization and for team members who have questions or concerns about privacy;
- supporting the Information Technology and Records Management teams in privacy-related service-provider-management matters;



- reporting regularly to the Executive Director, Legal Services on privacy practices and compliance matters;
- reviewing and updating the personal information inventory and recommending any necessary actions or revisions.

People Managers

People Managers are responsible for:

- familiarizing themselves with the requirements in FOIPPA, this policy and its associated procedures, and for ensuring that all team members they lead are made aware of their responsibilities under this policy;
- making a reasonable effort to ensure that the management of personal information by the team members that they lead meets the requirements of FOIPPA, this policy, and its associated procedures;
- contacting the Privacy and FOI Office should they have any questions about this policy; and
- reporting any suspected or actual breaches of FOIPPA, this policy, or its associated procedures, in accordance with the College's Privacy Breach Management Policy.

Team Members

All team members who collect, access, use, disclose, maintain and/or dispose of personal information are in a position of trust. All team members are responsible for:

- familiarizing themselves with the requirements of FOIPPA and this policy, and its associated procedures and complying with those requirements;
- treating all Personal Information to which they receive access in accordance with FOIPPA and this policy;
- only accessing the Personal Information that is necessary for the performance of their duties; and
- reporting any suspected or actual privacy breaches of FOIPPA, this policy, and any associated procedures in accordance with the College's Privacy Breach Management Policy.

Board and Committee Members

All Board and committee members who collect, access, use, disclose, maintain and/or dispose of personal information are in a position of trust. All Board and committee members are responsible for:

- familiarizing themselves with the requirements of FOIPPA and this policy, and its associated procedures and complying with those requirements;
- treating all personal information to which they receive access in accordance with FOIPPA and this policy;
- only accessing the personal information that is necessary for the performance of their duties; and
- reporting any suspected or actual privacy breaches of FOIPPA, this policy, and any associated procedures in accordance with the College's Privacy Breach Management Policy.



9. Limiting Collection of Personal Information

The College will normally collect personal information directly from the individual whom the information is about.

'Individual' may also include another decision maker authorized by law to act on behalf of the individual (such as a legal guardian or a person acting under a power of attorney).

When the College collects personal information directly from an individual, subject to exceptions permitted under FOIPPA, it will confirm to the individual:

- why it is collecting the information;
- the legal authority for collection; and
- the contact information of someone who can provide details about the collection and answer questions.

The College may collect personal information indirectly from sources other than the individual for the following reasons:

- to receive complaints respecting licensees and HPCs;
- to investigate a complaint about a licensee or HPC;
- when necessary to assess the competency of a person applying for registration (including renewal and reinstatement) with the College;
- to obtain examination results for exams administered by a third party;
- when necessary for the purposes of the College's quality assurance program;
- with the consent of the individual to whom the information relates; and
- where otherwise authorized or required by law.

10. Limiting Use and Disclosure of Personal Information

Team members may only access, use and disclose personal information when necessary to fulfill their role and as authorized by law.

The College uses and discloses personal information to fulfill the purposes it collected the information for, or for consistent purposes.

The College may also use and disclose personal information:

- for quality assurance and statistical purposes;
- for archival or historical purposes;
- in compelling circumstances that affect anyone's health or safety;
- in response to a court order, summons or subpoena;
- to the Ministry of Health (MOH) for the purposes of maintaining the [Provider and Location Register](#);
- to other health profession regulators when necessary to administer the College's registration, investigation, discipline, or quality assurance programs;
- to the public as authorized by the HPA for the purposes of maintaining the [license verification tool](#) and providing [Discipline Hearing Notices](#) and [Public Notices](#);



- to external auditors for the purposes of facilitating independent audits of the College's programs, activities and finances;
- to third-party service providers contracted to provide services to, or for, the College;
- for the purposes of establishing, managing or terminating an employment relationship;
- for other purposes, with the consent of the individual to whom the information relates; and
- as permitted or required by FOIPPA or as authorized or required by other law.

11. Storage and Retention

The College will retain personal information collected from individuals in accordance with FOIPPA and the College's Records Retention Schedule.

The College will retain personal information used to make a decision about an individual for at least one year.

The College aims to store personal information in Canada whenever reasonably possible. The College may store personal information outside of Canada if, after completing a Privacy Impact Assessment, the Registrar/CEO approves the storage outside of Canada.

The College uses reasonable security measures to destroy personal information at the end of its retention period so that the information cannot be reconstructed or recovered.

12. Accuracy and Individual Access

Accuracy

The College makes every reasonable effort to ensure that personal information is accurate and complete before using the information to make a decision that directly affects an individual.

In certain circumstances licensees are required to notify the College of changes to their personal information, including but not limited to the following:

- in the event of a legal name change;
- in the event of a change in address and phone number; and
- in the event of new charges and convictions that may be relevant to their registration.

Access and Correction

Individuals have a right to access personal information about themselves, subject to exceptions under FOIPPA. Access to personal information by applicants, licensees, and members of the public is provided in accordance with the College's Freedom of Information policies and procedures.

Individuals also have a right to request correction of personal information about themselves, if they believe there is an error or omission in the information.



If the College is permitted by FOIPPA to refuse to make a correction to an individual's Personal Information, the College will note the details of the request within the record(s).

Individuals other than College team members who wish to request access to or correction of their personal information, should contact the College Privacy and FOI Office at privacy@chcpbc.org.

Access by team members to their own employment personal information is provided in accordance with the College Team Members Handbook and related procedures.

Licensees and applicants may also update or access some personal information within their applicant/registrant portal.

13. Safeguards and Privacy Impact Assessments

The College completes a Privacy Impact Assessment (PIA) for proposed or significantly revised systems, projects, or activities involving Personal Information risks.

Team members who are leading systems, projects, or activities involving personal information must contact the Privacy and FOI Office and follow the processes established for PIAs.

The College applies reasonable security measures to protect personal information in College custody or control including:

- administrative safeguards (such as privacy and security policies and procedures, contracts or user agreements, and role-based access controls).
- physical safeguards (such as restricted office spaces, on-site security services and secure record or media device disposal).
- technical safeguards (such as personal information encryption, user activity logging and multi-factor authentication).

Any team members or Board or committee members making a decision or recommendation must treat the Personal Information of any individuals created, submitted, considered or investigated during that process as confidential in accordance with the provisions of the *HPA* and this policy.

When the College retains an external organization to undertake work on its behalf that involves the collection, use, disclosure or disposition of personal information, the College will enter into an agreement with that organization that requires the organization to protect personal information in accordance with FOIPPA.

14. Challenging Compliance, Privacy-Related Questions, Concerns and Complaints

Individuals are entitled to challenge the College's compliance with this policy.

Privacy and FOI Office

Team members who receive a complaint or inquiry about compliance with the policy must contact the Privacy and FOI Office.



Individuals may make a formal complaint or inquiry about compliance with this policy by contacting the Privacy and FOI Office.

CHCPBC Privacy and FOI Office

900 – 200 Granville St.

Vancouver, BC, V6C 1S4

Telephone: 1-877-742-6715

Fax: 1-604-608-9863

Email: privacy@chcpbc.org

<https://chcpbc.org/contact/>

Office of the Information and Privacy Commissioner

If the College's Privacy and FOI Office is unable to resolve a concern or complaint, the complainant may contact the Information and Privacy Commissioner of British Columbia.

Office of the Information and Privacy Commissioner for BC

PO Box 9038, Stn Prov Govt

Victoria, BC, V8W 9A4

Telephone: 1-800-663-7867

Fax: 1-250-387-1696

Email: info@oipc.bc.ca

www.oipc.bc.ca

15. Definitions

Contact information means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

Licensee means any individual registered or licensed with the College of Health and Care Professionals of BC.

Personal information means recorded information about an identifiable individual other than Contact Information.



16. Process Check

The following documents have been consulted and applied to this policy.

- Policy Development Framework (required)
- Anti-Discrimination Measures (S14/15 HPOA)
- The Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector* (February 2023)

Reviewed by the Board on:		<input checked="" type="checkbox"/> N/A
Reviewed by the Registrar/Deputy Registrar on:		<input checked="" type="checkbox"/> N/A
Date Approved 2025-09-19	Approved By <input type="checkbox"/> Board <input type="checkbox"/> Committee (<i>Name of Committee</i>) OR Name Dianne Millette Title Registrar CEO	
Date Effective 2025-10-01	Revision history	Last Updated: 2025-10-01
Next Review 2027-10-01		Previous Update:
Drafted by: Name Janina Kon		Title Executive Director, Legal Services