College of
HEALTH AND CARE
PROFESSIONALS OF BC

Policy	Replaces former policy:
Privacy Breach Management	☐ Title: ☒ N/A
	Date Effective: 2025-10-01
	Last Update:
Contact: Privacy and FOI Office	

Policy Statement

The College identifies, investigates, contains, reports and manages privacy breaches in accordance with the *Freedom of Information and Privacy Act* (FOIPPA), the *CHCPBC Privacy Breach Response Plan* (Appendix A) and any other applicable statutes, regulations, College bylaws, policies, and guidelines.

1. Policy Rationale and Purpose

The College is accountable for personal information generated or received in the course of its activities. It is subject to the specific legal obligations regarding identification, investigation, containment, reporting, and management of privacy breaches that are set out in FOIPPA.

Privacy breaches occur when this personal information has been lost, stolen or disclosed without authorization, whether accidentally or intentionally. Significant loss and harm to individuals and to the organization may result from privacy breaches that are not identified, investigated, contained, reported, and managed well.

The purpose of this policy is to ensure proper management of suspected and actual privacy breaches by:

- outlining the framework for the timely and effective identification, investigation containment, reporting, and management of suspected and actual privacy breaches, including confirming roles and responsibilities;
- promoting the College's compliance with FOIPPA; and
- confirming the roles and responsibilities of team members, Board and committee members and other relevant parties with respect to suspected and actual privacy breaches.

2. Policy Scope

The policy applies to all team members and Board and committee members and to all of the personal information in the College's custody or under its control.

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. Duties and Responsibilities

Executive Director, Legal Services

The Executive Director, Legal Services is responsible for overseeing the College's Privacy and FOI Programs and supervises the activities of the Lead, Privacy and FOI.

Lead, Privacy and FOI

The Lead, Privacy and FOI, in consultation with the Executive Director, Legal Services, is responsible for managing privacy breaches.

The Lead, Privacy and FOI consults with the IT Office when a suspected or actual privacy breach involves an information system.

The Lead, Privacy and FOI coordinates all communications regarding privacy breaches with the Office of the Information and Privacy Commissioner for British Columbia OIPC BC), under the direction of the Executive Director, Legal Services.

IT Office

The IT Office is accountable for managing security incidents involving information systems.

The IT Office supports the Lead, Privacy and FOI in managing a suspected or actual privacy breach that involves an information system.

People Managers

People Managers must ensure that their team members are made aware of their responsibilities under this policy.

People Managers are accountable for implementing mitigating actions if/when directed by the Legal Services/Privacy and FOI and/or the IT Office in response to a privacy breach.

Team Members

All team members are accountable for identifying and reporting actual or suspected privacy breaches to the Lead, Privacy and FOI at privacy@chcpbc.org, and if an information system is involved, also to the IT Office at ITsecurity@chcpbc.org.

Board and Committee Members

All Board and committee members are accountable for identifying and reporting potential or confirmed privacy breaches to the Lead, Privacy and FOI at privacy@chcpbc.org.

5. 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

6. Other Relevant Policies and Documents

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

- Privacy Policy
- 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

7. Key Partnerships

None identified at this time.

9. 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.

Personal information means recorded information about an identifiable individual other than *contact information*.

Privacy and FOI Office means the College Privacy and Freedom of Information Office.

10. 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:	☒ N/A
Reviewed by the Registrar/Deputy Registrar on:	☒ N/A

<table>
<tr><td>Date Approved
2025-09-19</td><td colspan="2">Approved By
☐ Board
☐ Committee (Name of Committee)
OR
Name Dianne Millette
Title Registrar/CEO</td></tr>
<tr><td>Date Effective
2025-10-01</td><td rowspan="2">Revision history</td><td rowspan="2">Last Updated:
Previous Update:
Previous Update:</td></tr>
<tr><td>Next Review
2027-10-01</td></tr>
<tr><td colspan="3">Drafted by: Name Janina Kon Title Executive Director, Legal Services</td></tr>
</table>

Appendix A

Privacy Breach Response Plan

Identifying a Privacy Breach

A privacy breach is a loss, theft or unauthorized access to Personal Information. Any disclosure of Personal Information outside the requirements of the job is also a Privacy Breach.

Some examples of privacy breaches include:

- loss or theft of information stored on a laptop, personal computer, portable storage device, network device, electronic media, or recorded on paper or on other written or printed media;
- unauthorized disclosure of Personal Information verbally or through an email to organizations or individuals outside of the College; and
- team members intentionally viewing more Personal Information than what is required to perform job responsibilities.

Team Member/Board and Committee Member Response to a Privacy Breach

Team Member/Board and Committee Members must follow three steps when responding to a privacy breach. If there is an actual or suspected privacy breach, the member will:

1. **Contain** the privacy breach immediately. (See *Containing a Privacy Breach*.)
2. **Report** the actual or suspected privacy breach to their people manager, a Director/Executive Director, or a Board/committee liaison and to the Privacy and FOI Office. (See *Reporting Actual or Suspected Privacy Breach*.)
3. **Assist** the Privacy and FOI Office in its investigation and follow-up, as required. (See I*nvestigation and Notification of Privacy Breaches*.)

Breaches may be simple or complex. This policy outlines the mandatory obligations for managing breaches; however, there is not a single path of step-by-step instructions. Each breach comes with variables for consideration, such as level of sensitivity, risk, liability and mitigation. Team Member/Board and Committee Members are required to seek the support of the Privacy and FOI Office in managing privacy breaches and in managing the associated risk to the College and information subjects.

Containing a Privacy Breach

Team Member/Board and Committee Members must act immediately to contain the privacy breach. This may include actions such as:

- stopping the unauthorized practice;
- recovering records;
- securing a system;
- correcting or enhancing physical security; and
- contacting the Privacy and FOI Office promptly for advice on containment.

Reporting an Actual or Suspected Privacy Breach

Team members and Board and committee members must report an actual or suspected privacy breach promptly to the Privacy and FOI Office. Team members and Board and committee members must make every effort to report within three hours of discovery.

If the actual or suspected privacy breach involves unauthorized access to an information system, team members and Board and committee members will also report the incident to the IT Office at ITsecurity@chcpbc.org.

Team members and Board and Committee members must immediately report to the Privacy and FOI Office actual or suspected privacy breaches involving sensitive information, such as any individually identifiable medical information, birthdate, or Social Insurance Number.

Team members and Board and Committee members must report the actual or suspected privacy breach via email to privacy@chcpbc.org and should specify:

- the date the incident occurred, if known;
- the date the incident was identified;
- a brief description of the incident, including the types of information involved, who the information was about (i.e. Registrant, Complainant, member of the public etc.), and who received the information; and
- any immediate steps taken to contain or manage the incident, if applicable. (See Containing the Privacy Breach)

Investigation and Notification of a Privacy Breach

The Privacy and FOI Office will promptly and thoroughly investigate the actual or suspected privacy breach and will take appropriate action to contain and mitigate risk arising from a privacy breach. The Privacy and FOI Office will collaborate with the IT Office in conducting the investigation and advising on privacy breach containment.

Members will assist the Privacy and FOI in its investigation. Upon request, a member will provide supporting documentation, assist in notifying affected individuals (if required) and assist in determining and implementing safeguards to prevent further/future incidents.

The Privacy and FOI Office will determine whether notification of the privacy breach must be made to the individual affected and/or to the Office of the Information and Privacy Commissioner for British Columbia (OIPC).

The Privacy and FOI Office will consider the following factors when deciding to notify impacted individuals or the OIPC:

- the sensitivity of the information;
- what harm might arise from the privacy breach, including whether it could be used for identity theft or other harmful purposes;
- the number of people affected and their relationship to CHCPBC
- whether the information could easily be exploited for reasons it was not intended for;
- the extent of any residual risks associated with the incident once it has been contained; and
- whether notification may cause harm to the individual affected by the privacy breach.