

## Interpretive Guideline - Privacy Legislation for Private Practitioners

Prc06/Policies.Int Gd – Priv Leg for PP.Oct 23-24 09

### **Introduction**

One of the duties and objectives for a college legislated under the *Health Professions Act* is to inform individuals of their legal rights, including privacy legislation.<sup>1</sup>

Public sector privacy legislation, affecting hospitals, health authorities and regulatory bodies, is found in federal legislation, the *Freedom of Information and Protection of Privacy Act* (FOIPPA) (1993).

Private sector privacy requirements are addressed in provincial legislation, the *Personal Information Protection Act* (PIPA) enacted on January 1, 2004. Registrants who consult with clients in a private practice setting must meet privacy requirements outlined in PIPA.

The key focus of all privacy legislation is the protection of personal information. This is defined as any identifiable information about an individual, including age and birth date, ethnic origin, race, financial and credit card information, wage or salary, home contact information, medical information, Social Insurance Number, religious and political affiliations, personal habits, preferences and activities, photographs and the contents of employee personnel files.

Personal information does not include the individual's name, business title, and business contact information. This is considered "public information." (Note: personal information published by an individual on their business card is considered public information.)

Personal information includes that gathered from clients, employee applications and employees.

### **Interpretation of PIPA for Private Practitioners**

The following table includes outlines ten principles of privacy legislation and recommended compliance actions for Registered Dietitian (RD) owners of private practices:

	<b>Privacy Principle</b>	<b>CDBC recommended compliance actions</b>
1.	Be accountable – ensure compliance with the legislation.	<ul style="list-style-type: none"><li>• Assume the role of 'privacy officer' – the person who is responsible for understanding the legislation and ensuring policies and processes are in place to protect the collection, use and disclosure of clients' and employees' personal information</li></ul>
2.	Identify purpose - before or at the time of collection, identify the purpose for collecting personal information	<ul style="list-style-type: none"><li>• State purposes in writing whenever personal information is requested</li><li>• Do not collect personal information if the purpose for collection cannot be stated</li></ul>

3.	Obtain consent – provide information and obtain consent for the collection, use and disclosure of personal information, including the consequences of consent not being provided	<ul style="list-style-type: none"> <li>• Prior to obtaining consent, ensure clients and employees understand who will have access to the information, how it will be used and when and how it will be disclosed</li> <li>• Obtain written or verbal consent; implied consent is given when clients and employees provide answers to posed questions</li> <li>• Consent may be withdrawn subject to legal reason and reasonable notice</li> </ul>
4.	Limit collection - collect only information that is required to fulfill the stated purpose	<ul style="list-style-type: none"> <li>• Review questions on forms for relevance and delete any not relevant to stated purpose</li> <li>• Identify optional questions</li> </ul>
5.	Limit use, disclosure and retention – use personal information and disclose it to another person only for the purpose it was collected; keep personal information only as long as needed	<ul style="list-style-type: none"> <li>• Limit use of personal information to the purposes stated; contact information must be used for business purposes only, not personal</li> <li>• Do not disclose an individual’s personal information to anyone unless written or verbal permission is obtained and recorded</li> <li>• Keep information only as long as needed for the purpose stated or as required by law</li> <li>• Shred paper records once usefulness is over; destroy discarded computer hard drives</li> <li>• In consultation with a lawyer, determine a retention period for client records and former employees’ files</li> </ul>
6.	Ensure accuracy - ensure personal information collected is complete, current and accurate as needed to fulfill stated purpose	<ul style="list-style-type: none"> <li>• Review and update personal information on a regular basis</li> </ul>
7.	Use safeguards – protect against unauthorized access, disclosure, use, copying or modification of all personal information, regardless of the format.	<ul style="list-style-type: none"> <li>• Keep all records (computer and paper) containing personal information safe from public view and from access by other clients</li> <li>• Do not discuss personal client and employee information in a public area</li> <li>• Allow employee access to client records on a “need to know” basis</li> <li>• Store records in lockable cabinets/drawers when not in use and at night; lock nightly</li> <li>• Back-up computer records regularly and store back-ups in a safe, unobtrusive place</li> <li>• Ensure computers have technological safeguards to protect against unauthorized access</li> </ul>

8.	Be open - communicate policies/practices	<ul style="list-style-type: none"> <li>• Publish a privacy policy for clients which includes information about accessing their personal records</li> <li>• Include a privacy statement on emails, computer and fax forms</li> <li>• Ask staff members to sign confidentiality statements</li> </ul>
9.	Provide individuals access - provide clients and employees access to their personal records on request to ensure accuracy and completeness	<ul style="list-style-type: none"> <li>• Write all health records in an objective and professional manner, following standards accepted by the profession</li> <li>• Develop a policy that enables employees and clients complete access to their personal file on request</li> </ul>
10	Provide a challenge process - provide a process for clients and employees to challenge compliance	<ul style="list-style-type: none"> <li>• Develop a process for monitoring the office's compliance with privacy legislation</li> <li>• Develop a clear and simple process to manage complaints about the office's privacy policy or access to information process</li> </ul>

**References**

- <sup>1</sup> *Health Professions Act*, section 16(2)(i)
- [Personal Information Protection Act](#)
- [Office of the Information and Privacy Commissioner for BC](#)
- Provincial government privacy legislation help line: 1.250. 356.1851