COLLEGE OF DIETITIANS OF BRITISH COLUMBIA

Interpretive Guideline - Privacy Legislation for Private Practitioners

Introduction

The key focus of all privacy legislation is the protection of personal information.

In the context of private practice clients, personal information is defined as any identifiable information about a client, including name, age and birth date, height, weight, sex, ethnic origin, race, financial and credit card information, wage or salary, home contact information, medical information, Social Insurance Number, religious and political affiliations, marital or family status, education, personal opinions, personal habits, preferences, photographs and employment information.

In the context of the private practitioner, personal information excludes information readily available to the public by mandate of the CDBC (legislated by the Health Professions Act (s.21)). This includes the registrant's name, contact information and place of business.

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. In accordance with privacy legislation, sections 70 and 71 in CDBC bylaws outline privacy requirements of registrants who have private practices. The Office of the Information and Privacy Commissioner provides independent oversight and enforcement of BC's access and privacy laws, including the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Information Protection Act (PIPA).

Public Sector Privacy

Public sector privacy legislation, affecting hospitals, health authorities and regulatory bodies, including dietitians working in these areas, is found in FIPPA legislation.

Private Sector Privacy

BC dietitians in private practice *within BC* are governed by the provincial legislation, PIPA.

BC dietitians in private practice *within BC, but who have clients across provincial boundaries* are subject to the Personal Information Protection and Electronic Documents Act (PIPEDA). All organizations that operate in Canada and handle personal information crossing provincial or national borders are subject to PIPEDA.

Interpretation of PIPA and PIPEDA for Private Practitioners

The following table includes outlines ten principles of privacy legislation and recommended actions for private practice Dietitians.

	Privacy Principle	CDBC recommended actions
1.	Be accountable – ensure compliance with the legislation.	• 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. This includes responsibility for contractors' records, which would apply for a

		dietitian who is the owner of a clinic and employs other contract dietitians or medical professionals. • Be aware of who your Ministry Privacy Officer is.
2.	Identify purpose - before or at the time of collection, identify the purpose for collecting personal information.	• State purposes in writing whenever personal information is requested • Do not collect personal information if the purpose for collection cannot be stated
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 (link below)	• 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. • Obtain written or verbal consent; implied consent is given when clients and employees provide answers to posed questions • Examples of implied consent in response to description of proposed nutrition intervention: o Nodding of the head o Keeping an appointment, voluntary answering of question related to nutrition history, submitting without objection to nutrition assessment and planned intervention. • Consent may be withdrawn subject to legal reason and reasonable notice • Understand that there are circumstances where consent is not required: o Urgent or emergency health care is required and the adult is incapable of making a decision o Involuntary psychiatric treatment is needed o Preliminary examinations such as triage are needed and, o Communicable diseases are involved.
4.	Limit collection - collect only information that is required to fulfill the stated purpose	• Review questions on forms for relevance and delete any not relevant to stated purpose. • Identify optional questions.
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	• Limit use of personal information to the purposes stated; contact information must be used for business purposes only, not personal. • Do not disclose an individual's personal information to anyone unless written or verbal permission is obtained and recorded. • Keep information only as long as needed for the purpose stated or as required by PIPA (1 year) and as set out in the CDBC Standards for Record Keeping (standard 5). • Shred paper records once usefulness is over; destroy discarded computer hard drives.

		• In consultation with a lawyer, determine a retention period for client records and former employees' files. • It is up to the registrant to know what Act/Law governs the allowance of the transfer/disclosure of personal information.
6.	Ensure accuracy - ensure personal information collected is complete, current and accurate as needed to fulfill stated purpose	• Review and update personal information on a regular basis if it will be used to make a decision affecting the individual.
7.	Use safeguards – protect against unauthorized access, disclosure, use, copying or modification of all personal information, regardless of the format.	• Keep all records (computer and paper) containing personal information safe from public view and from access by other clients. • Do not discuss personal client and employee information in a public area. • Allow employee access to client records on a "need to know" basis. • Store records in lockable cabinets/drawers when not in use and at night; lock nightly. • Back-up computer records regularly and store back-ups in a safe, unobtrusive place. • Ensure computers have technological safeguards to protect against unauthorized access.
8.	Be open - communicate policies/practices	• Publish a privacy policy for clients which includes information about management of personal information and accessing their personal records. • Include a privacy statement on emails, business websites, professional social media accounts, as well as computer and fax forms. • Ask staff members to sign confidentiality statements.
9.	Provide individuals access - provide clients and employees access to their personal records on request to ensure accuracy and completeness	• An individual's "Right of Access" includes: o Access to his/her personal information o An explanation of how the personal information is being used o Identifying to whom personal information has been disclosed • Write all health records in an objective and professional manner, following standards accepted by the profession. • Develop a policy that enables employees and clients complete access to their personal file on request.
10.	Provide recourse - provide a process for clients and employees to challenge compliance	• Develop a process for monitoring the office's compliance with privacy legislation

		• Develop a clear and simple process to manage complaints about the office's privacy policy or access to information process • If a complaint has been received about how an individual's personal information has been handled, contact the Privacy, Compliance and Training Branch.

Actions to be taken in the instance of a privacy breach

The majority of privacy breaches are due to human error. Take steps to (1) report, (2) recover, (3) remediate the breach, and (4) prevent future breaches.

To report a privacy breach, contact the Ministry Chief Information Officer by accessing the BC Government Privacy Breach website.

References

- Government of BC: Personal Information; accessed on October 8, 2019
- Health Professions Act, section 21; accessed on October 8, 2019
- Health Professions Act, section 16(2)(i); accessed on September 24, 2019
- Office of the Information and Privacy Commissioner for BC; accessed on September 21, 2019
- Freedom of Information and Privacy Protection Act (FIPPA); accessed on September 20, 2019
- Personal Information Protection and Electronic Documents Act (PIPEDA); accessed September 20, 2019
- Personal Information Protection Act (PIPA); accessed on September 20, 2019
- Ministry Privacy Officer Directory; accessed on September 23, 2019
- Provincial Legislation deemed substantially similar to PIPEDA; accessed on September 23, 2019
- CDBC Consent to Nutrition Guidelines; accessed on October 8, 2019
- Canadian Medical Protection Association (CMPA). Consent: A Guide for Canadian Physicians; accessed on November 18, 2019
- CDBC Standards for Record Keeping; accessed on September 25, 2019
- BC Government: Privacy Breach; accessed on September 24, 2019
- Provincial government privacy legislation help line; accessed on September 25, 2019