

Position Statement on the Protection of Privacy

Issued: June 5, 2019
Replaces: June 1, 2014

Purpose

The protection of personal information is an important principle to the BCAA and a legislated requirement (both provincially and federally) for itself and its members. The BCAA has a duty to protect the personal information of its members (and employees), while members have a duty to protect the information of their clients (and employees). The BCAA is committed to helping inform members of their responsibilities in the collection, use, disclosure and destruction of personal information related their professional activities, and to provide transparency in its own policy.

To better inform its members the BCAA has prepared guidelines (laid out below) for members to use in the development and implementation of business practices and policies related to their professional activities. Compliance with the four acts (PIPA-BC, FOIPPA, PIPEDA and CASL) is a requirement for kinesiologists and necessitates ongoing commitment to ensure knowledge remains up to date. It is recommended that members obtain legal advice pertaining to their unique business practices from a qualified lawyer should they have any specific concerns.

The BCAA makes available information about the policies and procedures it utilizes to handle personal information on its website (“terms of use” and “privacy statement”) and which is further detailed in the BCAA Corporate Privacy Policy. The BCAA has designated a Chief Privacy Officer to be accountable for the Association's compliance with the following key privacy principles related to the protection of personal information:

10 Key Privacy Principles

- 1) Accountability
- 2) Identifying purposes
- 3) Consent
- 4) Limiting collection
- 5) Limiting use, disclosure and retention
- 6) Accuracy
- 7) Safeguards
- 8) Openness
- 9) Individual Access
- 10) Challenging Compliance

Position Statement on the Protection of Privacy



BCAK Member Guidelines

Policies and Procedures for the Protection of "Personal" Information

GENERAL INFORMATION

Legislation

Public and private organizations in the province of British Columbia (BC) must comply with either the [Freedom of Information and Protection of Privacy Act \(FOIPPA-BC\)](#) or the [Personal Information Protection Act \(PIPA-BC\)](#) along with the [E-Health Act](#). These acts are monitored and enforced by the Office of the Information & Privacy Commissioner of BC. The Government of Canada also has legislation in force to protect the public from unwanted use of personal information, in the [Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#) and spam and other electronic threats in the Canadian Anti-Spam Legislation (CASL).

Freedom of Information and Protection of Privacy Act of BC (FOIPPA-BC)

Most public health care organizations (including hospitals, health authorities, MSP, PharmaNet, and the ministry of health) are subject to the privacy protection measures contained in BC's public sector privacy legislation, FOIPPA. The legislation guarantees the right of the public to gain access to, and request correction of personal information collected about them by public bodies and prevents the unauthorized collection, use, or disclosure of personal information by public bodies. FOIPPA does not apply to personal information collected by private organizations.

E-Health (Personal Health Information Access and Protection of Privacy) Act of BC

The E-Health Act allows for public health care bodies to create and maintain health information banks related to the operation and administration of the public health care system in BC. This act defines "personal health information" as any information related to an individual's health, the health care they receive and who provides their health care. The act primarily applies to government institutions and other laboratory/diagnostic facilities.

Personal Information Protection Act of BC (PIPA-BC)

Effective January 1, 2004 PIPA-BC came into force and applies to the majority of kinesiologists working within private practice. It requires all BC based businesses to comply with rules regarding the collection, use, disclosure and disposal of personal information. The core principle of PIPA-BC is that personal information is not to be collected, used, or disclosed without the prior knowledge and consent of the person (client) to which the information pertains subject to limited exceptions (e.g., where the collection, use, and disclosure is clearly in the

Position Statement on the Protection of Privacy

interests of the individual and consent cannot be obtained in a timely way and where the collection, use, and disclosure is necessary for medical treatment of the individual and the individual is unable to give consent or does not have the legal capacity to give consent). PIPA includes an implied consent provision, which applies to health care practitioners in most circumstances.

Other Legislation

Personal Information Protection and Electronic Documents Act (PIPEDA)

Individuals are also protected by PIPEDA which sets out regulations for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. The law gives individuals the right to access and, if applicable, request correction of the personal information these organizations may have collected about them. PIPEDA applies to personal information collected, used or disclosed by the retail sector, publishing companies, the service industry, manufacturers and other provincially regulated organizations. The Act does not apply to the personal information of employees of these provincially regulated organizations.

Canadian Anti-Spam Legislation (CASL)

Anti-Spam legislation is aimed at protecting Canadians from receiving unwanted electronic messages and other illegal or illicit activities related to or transmitted in conjunction with various forms of messaging services. From a business standpoint the regulations relating to the sending of commercial electronic messages (CEMs) are of particular significance and should be reviewed carefully.

General Data Protection Regulation (GDPR)

If you work at the international level with persons who are residents of a country in the European Union, you are subject the [General Data Protection Regulation](#). If this applies to you please take the appropriate steps to ensure compliance.

What is Personal Information?

Personal information is any information about an identifiable individual, excluding contact information and work product information. It includes an individual's gender, age, ethnic origin, race, identification numbers, financial and credit information, personal health information, consumer preference information, religious affiliations, donation history, travel history, personal habits, and personal history.

Position Statement on the Protection of Privacy

THE POSITION AND ROLE OF THE PRACTICING KINESIOLOGIST

Maintaining confidentiality is a fundamental responsibility of all Practicing kinesiologists and is a central part of the therapist-client relationship. The client ultimately owns his or her personal information (health and other). The kinesiologist acts as an accountable custodian of any medical information they collect by;

- Protecting its disclosure through appropriate consent and security means,
- Disclosing only what has been authorized, and
- Securely destroying information that is no longer required or has reached its retention limit.

Express consent, whether verbal or written should be obtained during the initial consultation and renewed annually or at an interval appropriate to the sensitivity of the information and can be confirmed during the course of providing direct client care/service. Informed consent for administrative purposes, such as billing is typically implied with respect to personal information but is recommended for all issues related to the gathering or sharing of personal health information. You may rely on and utilize the principle of implied/implicit client consent, however in doing so it is recommended information be made available on your website and/or in your office/place of business, through brochures for your clients on your business' or clinic's "Corporate Privacy Policy". Again, express consent should be obtained when requesting client information (records) from other health care providers or external sources.

Concerns expressed by clients to the kinesiologist about the collection, use or disclosure of personal (health or other) information should be brought to the immediate attention of the organization's designated Privacy Officer for investigation and follow up. The kinesiologist also needs to provide the complainant with information on how to contact the Chief Privacy Officer to discuss his or her concerns, as well as information on how to lodge a formal complaint with the Provincial or Federal Privacy Commissioner (see Challenging compliance "Principle 10" below).

Position Statement on the Protection of Privacy

The 10 Key Privacy Principles

Persons at all levels of a business organization must be committed to following the “10 Key Privacy Principles” and knowledgeable about the comprehensive policies and procedures described within this document as they apply to PIPA-BC and other related privacy legislation.

1. Accountability

Kinesiologists, and/or the organizations they work for, are responsible for the personal information under their control, both that of clients and employees. A privacy officer must be designated as responsible for the business organizations’ compliance with PIPA-BC. The privacy officer must understand what kind of information is covered under PIPA, its collection and protection. Contact information must be made available to the public (for example, on the business website): address, email and/or phone number. Members who are “self- employed” and operate as a “sole proprietor” must have their own privacy policy and are their own designated privacy officer.

Key functions of the privacy officer include;

- Helping clients understand what happens with their information,
- Developing and implementing the organization’s policies and procedures to protect personal information,
- Training employees about privacy policies, procedures, and confidentiality agreements,
- Responding to inquiries and complaints,
- Overseeing privacy practices, and
- Ensuring compliance with government legislation.

2. Identifying purposes

Before collecting personal information, kinesiologists and/or the organizations they work for must inform clients why they are collecting information and how it will be used. Each business organization should assess its information collection practices to define and document the purposes for which personal (health or other) information is collected. If it is not possible to identify the purpose, the kinesiologist/or organization should stop collecting the information.

Again, “Personal Information” (PIPEDA) is any information that relates to a natural person and allows that person to be identified (anonymized information, which cannot be matched to an individual, is not personal information). Information does not have to be recorded to be personal. Information requested about an individual but not recorded is still personal information and subject to regulation.

Position Statement on the Protection of Privacy

Information that is not considered personal information includes the name, title, and business contact information of clients and is therefore exempt from the protection of information policies and procedures (e.g. telephone numbers and office mailing address are not personal information, however business e-mail addresses, according to a recent finding by the Office of the Privacy Commissioner of Canada, are currently considered personal information). Other information related to business may be personal in nature such as income and would be covered by privacy policies and procedures to protect personal information.

3. Consent to the Collection, Use and Disclosure of Personal Information

Kinesiologists, and/or the organizations they work for are required to obtain client consent to collect, use, or disclose personal information, unless they can satisfy one of the limited exceptions to obtaining consent. Consent may be implied or expressly given; it may be given either verbally or in writing. To validate consent, clients must have a reasonable understanding of what information will be collected, who will have access to it, how it will be used, and to whom it may be disclosed. Clients should be able to withdraw consent at any time, subject to legal or contractual reasons and reasonable notice.

4. Limiting Collection

Kinesiologists, and/or the organizations they work for are only permitted to collect the minimum amount personal information that is necessary to fulfill the purposes of the person utilizing the services of the kinesiologist or organization. All information must be collected by fair and lawful means. Common sense dictates that “if you don’t need the information why would you collect it in the first place”.

5. Limiting Use, Disclosure and Retention

Kinesiologists and/or the organizations they work for must use and disclose personal information in accordance with the purposes communicated to the client. New uses and disclosures require new consent. Information can be kept only for as long as necessary to meet the original purposes, or as required by law. The use of detailed “release of information” forms is recommended whenever a client’s personal information is being requested from or released to any third party.

6. Accuracy

Client information must be accurately maintained and complete to fulfill the required purposes as indicated to the client.

7. Safeguards to Protect the Privacy of Personal Information

Kinesiologists and/or the organizations they work for must safeguard personal information to protect against security risks such as loss, theft, unauthorized disclosure, copying, use, or alteration. Technological safeguards

Position Statement on the Protection of Privacy



include the use of passwords and encryption. Security measures include the use of security clearances and limiting access to a "need-to-know" basis. Use of security safeguards that are appropriate to the sensitivity of the information, regardless of the medium in which client information is stored, is required.

8. Openness

Kinesiologists and/or the organizations they work for need to inform clients about the personal information they hold, the purposes for which it is used, other individuals or organization to which it is disclosed, and how an individual may access it.

9. Individual Access

Clients are entitled to access their personal information to ensure its accuracy and completeness, and to identify to whom it was disclosed, subject to certain exceptions. Organizations may charge a minimal fee for such access.

10. Challenging Compliance

Members of the public can challenge an organization's compliance with these principles by contacting the organization's "Chief Privacy Officer". Failing a satisfactory resolution, the Office of the Information and Privacy Commissioner (OIPC) of British Columbia may be contacted for organizations operating within BC and the Office of the Information and Privacy Commissioner of Canada for organizations that operate in more than one province or territory to file a formal complaint. Kinesiologists and/or the organizations they work for must respond in writing to all formal complaints within 30 days of receiving a "request for access" or they will be subject to possible fines and penalties levied by the OIPC.
