Privacy Guidelines

Community Living BC

December, 2010

Introduction

This Privacy Guide has been prepared by Community Living BC for the individuals it supports and their families, CLBC staff, and service providers. Its purpose is to help CLBC staff and service providers understand and carry out their privacy responsibilities and to let individuals and families know what they can expect in terms of their privacy and its protection. This Guide focuses on the *privacy of personal information*. It provides a general overview of important privacy legislation, and practices and policies endorsed by CLBC. This guide is not exhaustive and will not answer every question you may have. It has been designed to be used in conjunction with other materials and resources. Please note that the discussion in this Guide is for general information only and cannot be relied upon as legal or other advice.

The guide is divided into sections; each dealing with a different aspect of privacy. At the end of the Guide we have included a section on where to find more information and resources. This Guide is supported by CLBC's overarching privacy policy and specific policies such issues as information security, information systems access, confidentiality and information sharing.

You will see that some key words or phrases in this Guide are in italics. These words are explained in text boxes.

Privacy: the state or condition of being alone, undisturbed, or free from public attention as a matter of choice or right; seclusion, freedom from interference or intrusion.

Privacy of personal information: the fundamental right of individuals to determine for themselves when, how and to what extent their personal information is collected, used and communicated to others.

Legislation

In British Columbia there are two major pieces of privacy legislation that apply to personal information: the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*.

The Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) came into force in October 1993. The purpose of FOIPPA is to make public bodies more accountable and to protect personal privacy. The legislation covers all records in the custody or under the control of a public body. Public bodies include ministries, crown corporations, local government bodies, and self-governing professions, government agencies, boards and commissions, including CLBC. Any personal information you provide to CLBC is collected, used and disclosed in accordance with FOIPPA.

Personal Information Protection Act

British Columbia's *Personal Information Protection Act* (PIPA) came into force on January 1, 2004. PIPA applies to all private sector organizations including businesses, non profits and unions. The legislation contains rules to protect the privacy of personal information collected, used and disclosed by these organizations as well as limited access provisions to allow individuals to obtain access to their own personal information. Non profit agencies and private providers of community living services are covered by PIPA for those aspects of their operations that are not specifically related to services for individuals supported by CLBC.

Oversight of FOIPPA and PIPA rests with the Information and Privacy Commissioner of BC.

Comparing PIPA and FOIPPA

There are three notable differences between PIPA and FOIPPA:

Storage and Access: PIPA does not include the FOIPPA provisions regarding storage of and access to personal information outside Canada. As long as personal information is managed in accordance with the requirements of PIPA it does not matter where the data is or where it is accessed from.

Contact Information: FOIPPA and PIPA exclude business contact information from the definition of personal information.

Consent: PIPA requires consent for the collection, use and disclosure of personal information; service providers should familiarize themselves with the criteria which allows specific exemptions to be made. It is up to the organization to determine whether the form of the consent is explicit (written or verbal) or deemed (implied). FOIPPA does not use the term *consent* for the collection of information although that authority exists for the *use and disclosure* of information. However, CLBC, like most public bodies, must notify individuals when it is collecting personal information, e.g., when an individual applies for services and provides information on their age, eligibility, family contact, etc.

As service providers are subject to the FOIPP Act when under contract to and providing service on behalf of CLBC, each contract includes references to privacy protection requirements. In addition CLBC is introducing a Privacy Protection Schedule. The purpose of this schedule is to ensure that contractors and service providers are aware of and comply with their statutory obligations under FOIPPA. .

Privacy Protection Schedule

The Privacy Protection Schedule includes rules for the collection of personal information, the accuracy and correction of this information, the protection, storage, retention of personal information, and its use and disclosure. The schedule also requires service providers and contractors to notify CLBC of any unauthorized disclosure of personal information and allows CLBC with reasonable notice to inspect any personal information in the possession of the contractors or any of the contractor's information management policies or practices related the management of personal information.

A complete copy of the Privacy Protection schedule can be found at CLBC's website. http://www.communitylivingbc.ca/

In summary PIPA applies to any private sector records a contractor creates outside of the contractual relationship with CLBC, FOIPPA for records created under or as a result of the contractual relationship with CLBC.

Accountability and Monitoring

There are a number of ways adherence to BC's privacy legislation is monitored. The accreditation process for CLBC's large service providers includes standards relating to privacy policy and practice. Accredited agencies must demonstrate their compliance in order to maintain their accreditation. For smaller, non-accredited agencies compliance with privacy requirements is covered in service standards and is an element of CLBC's monitoring framework.

Individuals may use the CLBC Complaints Process (please see http://www.communitylivingbc.ca/what_we_do/documents/complaintsresolution.pdf) if they believe their privacy rights have been violated and the issue cannot be resolved by the facilitator or analyst involved. If the Manager is unable to resolve the complaint or the individual is not satisfied with the response they can take their complaint to the Director of Regional Operations for their region and then to CLBC's Director of Quality Assurance and finally to the Chief Executive Officer.

Individuals also may complain to the Office of the Information and Privacy Commissioner if they consider their personal information has not been collected, used or disclosed in compliance with FOIPPA requirements, that their personal information held by CLBC or service providers is not accurate or complete, or that their request for access or correction has not been handled properly.

The Office of the Information and Privacy Commissioner investigates, mediates and attempts to resolve appeals concerning access to information disputes, and where necessary issues binding orders. The Office generally requires a complainant to first work out a solution directly with the organization involved, without their involvement. The Office will mediate a settlement of any complaint that it does accept.

The Office of the Information and Privacy Commissioner can also comment on the access and privacy implications of proposed legislation, programs or policies and on the privacy implications of new technologies or data matching schemes.

Roles and Responsibilities

The Director, Quality Assurance is CLBC's Privacy Officer and has overall responsibility and accountability for privacy. The Director is the focal point for privacy compliance related activities, providing leadership for CLBC's privacy commitment, liaising with the external agencies with respect to privacy issues, working with service provider accreditation bodies on any privacy related issues, negotiating any information sharing agreements with third parties, reviewing research related requests for access to personal information, and receiving and responding to complaints or inquiries about CLBC's personal information practices.

The Director is supported in this role by CLBC's Cross Functional Privacy Compliance Committee who:

- Oversees the development and implementation of corporate privacy policies and procedures
- Ensures consistency and standardization of privacy policies and procedures,
- Assigns privacy roles and responsibilities across the organization,
- Ensures Privacy Impact Assessments are performed for key CLBC change initiatives that may have a privacy impact,
- Monitors CLBC's privacy commitments
- Communicates with internal and external stakeholders on privacy issues.

Representatives of CLBC's Human Resources, Information Technology, Quality Assurance, Communications, Regional Operations, Strategic Planning, Organizational Development, Corporate Services and Policy and Program Development Divisions are members of the Committee.

Information Access Operations Branch in the Ministry of Citizens' Services is responsible for the management of records within ministries' control and/or custody and for ensuring the BC Government meets its access obligations under the FOIPPA. The Branch provides freedom of information request processing, related advice and training services for CLBC. Any policy advice re the act is provided by Knowledge and Information Services in Citizens' Services.

Personal Information

Collection of personal information

Information for purposes of this Guide and in compliance with FOIPPA means "personal information" recorded about an identifiable individual.

Personal information includes, but is not limited to:

- name, address, telephone number, email
- race, national/ethnic origin, colour, religious or political beliefs or associations
- age, sex, sexual orientation, marital status
- identifying number or symbol such as social insurance number or driver's licence number
- fingerprints, blood type, DNA prints
- health care history
- educational, financial, criminal, employment history and
- anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else.

Personal information also includes separate pieces of information that may seem unrelated, but when put together would allow someone to accurately infer information about an individual.

CLBC and service providers need to collect personal information to operate programs and provide community living services. When doing this CLBC and service providers should only collect personal information that is necessary for the provision of a particular service, directly from the individual the information is about and after telling that individual the purpose and the legal authority for collecting it and the title, business address and business telephone number of the person designated to answer questions about the collection of personal information. Whenever possible, personal information should be collected directly from the individual.

Each new CLBC employee is advised at the time of employment via a personal information collection and use clause on the application form and the offer letter of the expected uses of their personal information.

CLBC staff must use an individual's personal means of communicating when advising that they are collecting information and why or when obtaining consent to share information. Individuals may involve family, friends, advocates or members of a personal support network to assist them in making decisions and give informed consent.

Informed Consent: A person is made aware of the decision or choice to be made, understands the possible consequences of giving and not giving consent, including for instance the purpose for which released information may be used and consents voluntarily.

Accuracy of personal information

CLBC and service providers must make a reasonable effort to ensure that personal information collected by or on behalf their agencies is accurate and complete if it is likely that this personal information will be used to make a decision that affects that individual or it is likely the personal information will be disclosed to another organization. These rules help prevent the use of incorrect information to make a decision about an individual and the possible disclosure of incorrect personal information to another organization.

Correcting personal information

Individuals have a right to ask CLBC and service providers to correct their personal information if they believe that their records contain factual errors or omissions. These agencies must correct any factual error or omission and inform other organizations to whom they have disclosed the incorrect information. If CLBC or a service provider decides that there is no factual error or omission they must still annotate the record with the requested correction. If an individual is not satisfied with the decision they can ask the Office of the Information and Privacy Commissioner to review the matter.

In addition service providers whose contracts include the Privacy Protection Schedule must correct or annotate the personal information of an individual within five business days of receiving a written direction from CLBC. Within five days of correcting or annotating any personal information the service provider must provide the newly corrected or annotated information to any party that it had disclosed or shared the personal information within the last year. Finally if the service provider receives a request for correction of personal information from someone other than CLBC the service provider must promptly advise that person to make the request to CLBC and provide the contact information of the CLBC staff member to whom such requests are made.

Sharing of Personal Information

Individuals supported by CLBC have the right to expect that CLBC staff and service providers will be bound by *confidentiality* and that their personal information will be securely stored and only used for the purposes for which it was collected.

Confidentiality: the obligation to keep others personal information private or secret and safe from access, use or disclosure by people who are not authorized to have that personal information.

Sharing Personal Information with Consent

Personal information will only be shared with CLBC staff and service providers with an individual's informed consent, on a *need to know* basis and for *consistent purposes* as outlined in FOIPPA.

Need to Know: the legitimate requirement to know, access or possess personal information that is critical to the performance of an authorized, assigned mission.

Consistent Purposes: Use and disclosure of personal information is considered consistent if the use and disclosure has a reasonable and direct connection to the purpose for which it was originally collected and is necessary to carry out the mandate and responsibilities of CLBC.

An example of consistent use would be if a community living organization wished to evaluate the effectiveness of one of its programs. They use the personal information they have collected from the individuals they support in this program to determine its effectiveness compared with other programs and approaches. The use of this information for evaluation is considered consistent with the original purpose for which personal information was collected. An example of non consistent or improper use would be if the organization used the information for a second, totally unrelated purpose; for example to fund raise for a new facility.

Sharing Personal Information without Consent

There are limited circumstances in which an individual's personal information can be shared without their consent. Personal information can be shared without consent in the following circumstances:

- When required by law, on receipt of a Court order such as a subpoena;
- As required to the Medical Health Officer when an individual may have a serious communicable disease;
- To assist a Medical Health Officer to investigate alleged abuse or neglect in licensed facilities;
- As required under the Adult Guardianship Act;
- As required to the Ombudsperson under the Ombudsperson's Act;
- As required to the Coroner under the Coroners Act;
- Financial and health records to the Public Trustee as required under the Public Guardian and Trustee Act.

Personal information can also be shared without consent

- In compelling circumstances where the health and safety of individuals may be impacted.
- To assist police in an ongoing investigation where there is a significant likelihood of harm to the safety of an individual or the public.

Sharing of Third Party Records

CLBC staff and service providers must not share personal records about an individual that have been obtained in confidence from a third party (a person or organization other than the person or organization requesting the information). The third party is responsible for release of their records.

Access

Individuals have a right to be given access to their own personal information, to know how their information has been used and whether and to whom their information has been disclosed.

Individual access requests for personal information held by CLBC are made directly to the Information Access Operations Branch in the Ministry of Citizens' Services which manages the response and provision of records on behalf of CLBC.

Service providers are expected to have procedures in place to guide their response to an individual's request for access to their personal information. If there is any question as to what information is acceptable to share such as CLBC documents or third party assessments the individual should be advised to make the request to the Information Access Operations Branch (IAO). IAO is a branch under Services B.C, Ministry of Citizens' Services which manages all requests for information under the Freedom of Information and Protection of Privacy Act (FOIPPA) for the Province of B.C. The

Information Access Operations Branch is legislated under that act to provide a response to an access request within 30 business days.

Denial of Access

Access to one's own personal information can in rare and exceptional circumstances, be refused if disclosure would:

- harm someone else
- harm an investigation or legal proceeding
- disclose someone else's personal information or
- disclose confidential business information

If an individual is not satisfied with what is disclosed they can ask the Office of the Information and Privacy Commissioner to review the response.

Disclosure for Research or Statistical Purposes

FOIPPA covers records created by service providers under their contractual relationship with CLBC. Under FOIPPA and CLBC's implementation requirements CLBC and its service providers may disclose personal information about individuals supported by CLBC for research and statistical purposes only if the following conditions are met:

- CLBC has approved the proposed purpose, scope and outcome of the research and specific methodology to be used, ensuring that relevant aspects of FOIPPA are addressed and in particular that the research purpose cannot be reasonably accomplished unless the personal information is provided in individually identifiable form.
- Any record linkage is not harmful to the individuals supported and the benefits are clearly in the public interest.
- The Director of Quality Assurance, CLBC has approved conditions related to the security and confidentiality, removal and destruction of individual identifiers at the earliest reasonable time and prohibited any subsequent use or disclosure without the expressed authorization of CLBC.
- The researcher or statistician to whom the information is disclosed has signed an agreement to comply with these conditions, FOIPPA and CLBC's policies and procedures relating to the confidentiality of personal information.
- Disclosure for research purposes is authorized in Canada only

Retention of Personal Information

FOIPPA requires CLBC to retain personal information for one year if it is used to make a decision directly affecting the individual. This minimum retention period gives individuals a reasonable opportunity to obtain access to the personal information when it has been used to make a decision affecting them.

CLBC however retains information beyond what is required in FOIPPA if it is needed to provide programs and services. CLBC records that contain personal information and service provider records which contain personal information on an individual created as a result of a contractual relationship with CLBC must be retained for *seven* years following the last date service was provided to that individual. If a service provider goes out of business, the files must be transferred to CLBC. The same seven year retention period applies.

Maintaining personal information that is no longer useful is a security liability. When all relevant retention requirements have been met and the personal information is no longer relevant for providing programs and services, the information is archived or destroyed in a manner that will not compromise security or privacy of the information.

Security of Personal Information

It is important to secure personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal. CLBC uses both physical and electronic safeguards to secure personal information.

Physical safeguards include the use of locked filing cabinets, limiting material on desks, counters, meeting room tables, proper use of fax machines and copiers, physically securing offices where personal information is held, and encouraging a clean desk policy for employees who handle personal information.

All CLBC employees who work with personal information outside the workplace must have prior approval to work with this type of information off site to ensure that the protection, security and storage requirements of FOIPPA are met. In these circumstances the CLBC staff member is personally responsible for protection of the information while off site.

Service providers must also protect personal information by making reasonable security arrangements.

In terms of electronic safeguards, CLBC uses computer systems to support its programs and services. Access to the personal information in these computer systems is based on clearly defined roles that are associated with positions in CLBC. Standard roles are

defined and assigned for common positions. The roles are appropriate to the responsibilities of each position and consistent with requirements for information security, confidentiality and privacy.

Access is on a need-to-know basis, so that users access only the specific information needed to carry out their responsibilities. Access is not provided to a user until authorization procedures are completed and users are aware of their assigned roles and sign a usage agreement.

CLBC staff are required to limit the transmission of personal information within email and email disclosure of personal information over unencrypted emails outside of the CLBC computer network is not permitted. Staff are required to use a secure method of transmission. Email is a record and all email residing on CLBC computer equipment are subject to requests and privacy protection under FOIPPA.

Breaches

Breaches occur when unwanted or unexpected events such as theft, loss or unauthorized disclosure threaten the privacy of personal information. If a breach occurs CLBC staff are required to report it immediately to their supervisor to minimize potential impact of the breach. CLBC staff members must contain the breach if possible by recovering the information or records; suspending the activity that led to the breach, or correcting any physical or systems weakness that may have led to the breach.

In the case of service providers; they are required to immediately notified CLBC in the event of unauthorized disclosure of personal information. CLBC uses an established breach protocol to assess the extent and impact of the breach including the personal information involved, cause and extent of the breach, individuals affected, and foreseeable harm. CLBC will notify affected individuals if necessary.

Additional Resources

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) can be found here:
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_07

More information and resources, including the FOIPPA Policy Manual prepared by the Office of the Chief Information Officer can be found here:
http://www.cio.gov.bc.ca/cio/priv_leg/foippa/index.page

The *Personal Information Protection Act* can be found here:
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

There are useful templates and policy documents re PIPA on the OCIO site in government.
A guide for businesses and organizations to BC's *Personal Information Protection Act* prepared by the Office of the Information and Privacy Commissioner can be found here:
http://www.oipc.bc.ca/pdfs/private/a-_GUIDE_TO_PIPA(3rd_ed).pdf