Privacy Procedures for the Surrey-North Delta Division of Family Practice

The Surrey-North Delta Division of Family Practice is subject to the BC **Personal Information Protection Act** with respect to their collection, use, disclosure and retention of personal information.

The Surrey-North Delta Division of Family Practice collects, uses, and discloses personal information about individuals to:

- provide and administer services to its clients
- develop, manage, protect, and improve its services
- conduct customer satisfaction surveys,
- comply with legal requirements and
- manage its operations

Privacy Procedures

These procedures support the ten interrelated principles that form the basis of the organization's Privacy Policy.

1. Assign Accountability

The organization is responsible for personal information under its custody and/or control and has designated an individual who is accountable for its compliance.

1.1. Accountability for the organization's compliance with the principles rests with the designated Privacy Officer, even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual.

1.2. The identity of the individuals designated by the organization to oversee its compliance with the principles is made known.

1.3. The organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization uses contractual or other means to provide a comparable level of protection while the third party is performing the processing.

1.4. The organization has implemented policies and procedures to give effect to the principles, including:

1.4.1. Protection of personal information,
1.4.2. Response to complaints and inquiries,
1.4.3. Breach notification and reporting,
1.4.4. Staff training and
1.4.5. Guidance to comply with its policies and procedures.

2. Identify Purposes for Collecting Personal Information

The organization identifies the purposes for which it collects personal information at or before the time the information is collected.

2.1. The organization documents the purposes for which it collects personal information in order to comply with Openness (Clause 8) and Individual Access (Clause 9).

2.2. Identifying the purposes for which personal information is collected at or before the time of collection allows the organization to determine the information it needs to collect to fulfill these purposes. Limiting Collection (Clause 4) requires the Organization to collect only that information necessary for the identified purposes.

2.3. The identified purposes are specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An agreement or a notice, for example, can give notice of the purposes.

2.4. When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.

2.5. Persons collecting personal information for the organization are able to explain to individuals the purposes for which the information is being collected.

3. Obtain Consent to Collect, Use and Disclose Personal Information

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected as required or authorized by law, seeking the consent of the individual might defeat the purpose of collecting the information.

3.4. Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, the organization seeks consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when the organization wants to use information for a purpose not previously identified).

3.5. The principle requires "knowledge and consent." The organization will make a reasonable effort to ensure the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes will be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

3.6. The organization does not, as a condition of the supply of a service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

3.7. The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, the organization will take into account the sensitivity of the information.

3.8. In obtaining consent, the organization also takes account of the reasonable expectations of the individual.

3.9. The ways in which the organization seeks consent may vary, depending on the circumstances and the type of information collected. It generally seeks express consent when the information is likely to be considered sensitive. Implied consent is generally appropriate when the information is less sensitive.

3.10. Individuals can give consent in many ways. For example:

- 3.10.1. A notice may be used to seek consent, collect information and inform the individual of the uses that will be made of the information. By completing and signing a form, the individual is giving consent to the collection and the specified uses,
- 3.10.2. Individuals may request that their names and addresses not be given to other organizations or used for marketing purposes,
- 3.10.3. Consent may be given orally when information is collected over the telephone, or
- 3.10.4. Consent may be given at the time that individuals use a service.

3.11. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization will inform the individual of the implications of such withdrawal.

4. Collect Only Necessary Personal Information

The organization collects only the personal information necessary for the purposes it has identified. It collects information by fair and lawful means.

4.1. The organization does not collect personal information indiscriminately. It limits both the amount and the type of information collected to that which is necessary to fulfill the purposes identified. The organization specifies the type of information collected as part of its information-handling policies and practices, in accordance with Openness (Clause 8).

4.2. The requirement that personal information be collected by fair and lawful means is intended to prevent the organization from collecting information by misleading or deceiving individuals about the purposes for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

5. Limit Use, Disclosure, and Retention of Personal Information

The organization does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law. The organization retains personal information only as long as necessary for the fulfillment of those purposes.

5.1. If considering using personal information for a new purpose, the organization will obtain consent (see Clause 3) and document this purpose (see Clause 2.1).

5.2. The organization has developed guidelines and implemented procedures with respect to the retention of personal information. These guidelines include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual will be retained long enough to allow the individual access to the information after the decision has been made. The organization is subject to legislative and regulatory requirements with respect to retention periods.

5.3. Personal information that is no longer required to fulfill the identified purposes is destroyed, erased, or made anonymous. The organization has developed guidelines and implemented procedures to govern the destruction of personal information.

6. Ensure Accuracy of Personal Information

Personal information is as accurate, complete, and as up-to-date as is necessary for the purposes for which it is to be used.

6.1. The extent to which personal information is accurate, complete, and up-to-date depends upon the use of the information, taking into account the interests of the individual. Information will be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

6.2. The organization does not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

6.3. Personal information that is used on an ongoing basis, including information that is disclosed to third parties, will generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

7. Implement Safeguards for Personal Information

The organization protects personal information by security safeguards appropriate to the sensitivity of the information.

7.1. The security safeguards protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The organization protects personal information regardless of the format in which it is held.

7.2. The nature of the safeguards varies depending on the sensitivity of information that the organization has collected, the volume, distribution, and format of the information and the method of storage. More sensitive information will be safeguarded by a higher level of protection.

7.3. The methods of protection include:

7.3.1. Physical measures (e.g., locked filing cabinets and restricted access to offices),
7.3.2. Organizational measures (e.g., limiting access on a "need-to-know" basis) and
7.3.3. Technological measures (e.g., the use of robust passwords and encryption).

7.4. The organization makes its representatives, employees, and contract staff aware of the importance of maintaining the confidentiality of personal information.

7.5. Care is used in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information (see Clause 5.3).

8. Publish Personal Information Policies and Practices

The organization makes readily available to individuals specific information about its policies and practices relating to the management of personal information, most notably on its web site.

8.1. The organization is open about its policies and practices with respect to the management of personal information. Individuals are able to acquire such information without unreasonable effort. This information is made available in a form that is generally understandable.

8.2. The information made available includes the:

- 8.2.1. Name or title, and the address, of the persons who are accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded,
- 8.2.2. Means of gaining access to personal information held by the organization,
- 8.2.3. Type of personal information held by the organization, including a general account of its use,
- 8.2.4. Reference to a web site that explains the organization 's policies, standards, and procedures and
- 8.2.5. Personal information that is made available to related organizations (e.g., business partners and service providers).

8.3. The organization makes information on its policies and practices available in a variety of ways. For example, it may choose to make brochures available in its places of business, mail information to its clients, and provide online access.

9. Provide an Individual Access to Their Personal Information

Upon request, an individual will be informed of the existence, use, and disclosure of his or her personal information and will be given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

In certain situations, the organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement are limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

9.1. Upon request, the organization will inform an individual whether or not it holds personal information about the individual and the sources of this information. It will allow the individual access to this information. In addition, the organization will provide an account of the use that has been made, or is being made, of this information and an account of the third parties to which it has been disclosed.

9.2. An individual may be required to provide sufficient information to permit the organization to provide an account of the existence, use, and disclosure of personal information. The information provided will only be used for this purpose.

9.3. In providing an account of third parties to which it has disclosed personal information about an individual, the organization will be as specific as possible.

9.4. The organization will respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation will be provided.

9.5. When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization will amend the information as required. Depending upon the nature of the information challenged,

amendment may involve the correction, deletion, or addition of information. With consent, the amended information will be transmitted to third parties having access to the information in question.

9.6. When a challenge is not resolved to the satisfaction of the individual, the organization will record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

10. Implement Procedures to Challenge Compliance

An individual is able to address a challenge concerning compliance with the organization's Privacy Policies and Procedures to the Privacy Officer and to the BC Information and Privacy Commissioner.

10.1. The individual accountable for the organization's compliance may be contacted by sending an email to the Privacy Officer Susan Kreis.

10.2. The organization has procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures are easily accessible and simple to use.

10.3. The organization informs individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures.

10.4. The organization investigates all complaints. If a complaint is found to be justified, it will take appropriate measures, including, if necessary, amending its policies and practices.

These privacy procedures are based on Schedule 1 of the federal Personal Information Protection and Electronic Documents Act (PIPEDA), which is, in turn, based on the Canadian Standards Association's Model Code for the Protection of Personal Information. The organization is subject to British Columbia's Personal Information Protection Act (PIPA), which the federal government has deemed to be substantially similar to PIPEDA. The organization is also subject to independent oversight by the BC Information and Privacy Commissioner www.oipc.bc.ca.

These Privacy Procedures are to be read in conjunction with the associated Privacy Policy. Questions about these Privacy Procedures can be directed to the Privacy Officer Susan Kreis.