Getting Ready for Privacy Legislation

GUIDE

Privacy Requirements and Policies for Health Practitioners

PUBLISHED BY THE COLLEGE OF CHIROPRACTORS OF ONTARIO
NOVEMBER 2003

This booklet is not intended to provide legal advice. It provides some practical suggestions for how some organizations can review their information handling practices and develop a Privacy Policy. The *Personal Information Protection and Electronic Documents Act* is unclear in a number of areas and is enforced by the federal Information and Privacy Commissioner. Thus, the descriptions provided below are based on current information and may change as experience with the legislation and its enforcement develops. Some provisions in the Act are simplified for the purpose of identifying issues for consideration. For legal advice, please speak to your own lawyer.

Adapted from the work of:
Richard Steinecke
Steinecke Maciura LeBlanc
Barristers & Solicitors

INDEX

Page

Introduction

The following document is a simplified, abbreviated and practical description of the requirements of the Personal Information Protection and Electronic Documents Act (PIPEDA). The unique combination of features contained in this checklist is as follows:

- ✓ *a brief, plain language description of the major requirements of the legislation (which does not attempt to be exhaustive)*
- ✓ *organization of the information in an order that helps the reader prepare the required Privacy Policy for the organization*
- ✓ *step-by-step checklists (see accompanying Checklist document) of the requirements and suggestions needed to prepare the required Privacy Policy for the organization*
- ✓ *concrete examples (with emphasis on those appropriate for the health practitioners)*
- ✓ *sample forms*

The emphasis in this document is to help small health offices or other organizations to bring themselves into compliance with PIPEDA. Large organizations may require and have the resources for a formal data flow analysis, extensive assistance by external consultants and a large team of people to balance the competing priorities of different departments. However, there are few practical tools available for small health offices or other organizations.

Completing the checklists will assist an organization to comply with the requirements of PIPEDA. Boxes "☐" are to be ticked off when appropriate and blanks "_____" are to be filled in where they apply to your organization.

There are six steps to both this Guide and the accompanying Checklist document:

1. *Designating Your Organization's Information Officer*
2. *Information and Activities Covered by the Privacy Plan*
3. *Collecting Personal Information*
4. *Safeguards, Retention and Destruction*
5. *Access, Corrections, Complaints and Openness, and*
6. *Implementing Your Privacy Plan*

A list of the forms attached to this Guide is as follows:

Form 1 – Health Consent Form
Form2 – Privacy Policy – Generic Form
Form 3 – Privacy Policy - Health Practitioner Sample Form

Step 1 – Designating Your Organization's Information Officer

(a) Identifying Your "Organization"

Often it is obvious who or what your organization is. An organization can be:

- ✓ *a single individual (e.g., in a sole proprietorship)*
- ✓ *a partnership*
- ✓ *a corporation*
- ✓ *an association of individuals, partnerships and/or corporations*

Where a number of persons or entities work together, they may choose either to treat themselves as a single "organization" for the purposes of developing one Privacy Policy, or to require each one to develop their own Privacy Policies (e.g., a multidisciplinary office). Similarly, where consultants (e.g., lawyers, accountants, information technology advisors) or outsourced agencies (e.g., database management, marketing, office cleaners, office security, file storage) are used, there may again be a choice as to whether or not to treat them as a part of a single organization.

The advantages of treating various persons or groups as one organization includes the following:

- ✓ *the simplicity of having a single set of rules for everyone*
- ✓ *avoiding the need to enter into contracts with everyone outside of the organization who has access to personal information on your behalf*
- ✓ *simplifying the consent required from those who provide personal information*

The disadvantages of treating various persons or groups as one organization includes the following:

- ✓ *having to monitor the information handling practices of consultants and agencies*
- ✓ *reluctance of consultants and agencies who have multiple clients to be bound by multiple privacy plans*

(b) Selecting Your Information Officer

In order to comply with the Personal Information Protection and Electronic Documents Act (PIPEDA), each organization must designate an individual (or individuals) who is accountable for the organization's compliance with the privacy obligations. Specific tasks that this "Information Officer" (sometimes called a "Privacy Officer") is responsible for include the following:

- ✓ *reviewing the organization's collection, use and disclosure of personal information*
- ✓ *implementing procedures to protect personal information*
- ✓ *being the contact person for client or public inquiries about information handling*
- ✓ *establishing and, in a small organization, operating a complaints procedure*
- ✓ *training and continually updating staff on information Privacy Policy*
- ✓ *monitoring compliance*
- ✓ *publishing the organization's information handling policies to the public*

Characteristics of a good Information Officer include the following:

- ✓ *a senior position in the organization*
- ✓ *familiarity with how information is collected, stored, used and disclosed in the organization*
- ✓ *experience with human resources or personnel management*
- ✓ *experience with customer relations*
- ✓ *a comfort level with legal matters*

The Information Officer need not be an employee of the organization. It can be the organization's lawyer or an outside privacy consultant. However, for many small offices, it makes sense for the Information Officer to be the owner, senior partner or president.

Step 2 – Information and Activities Covered by the Privacy Plan

The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to any "commercial activities" of the organization that involve "personal information". It is important to first identify what commercial activities your organization engages in and what personal information it collects, uses and discloses in the course of those activities. Only then can you go to the next step of assessing whether your current information practices require change.

(a) Commercial Activities

The term "commercial activities" is vague and it is unclear as to precisely how far it goes. Little help has been provided to assist those who might be covered by PIPEDA and commentators have taken widely divergent views. Likely, if the organization is non-profit in nature, PIPEDA only applies to activities of the organization that are commercial in nature (e.g., selling or bartering client or membership information, fund raising ventures). However, if the organization is for profit in nature (e.g., a private practice), then almost everything done by the organization is a commercial activity. This is probably true even if the activity is publicly financed (e.g., paid by OHIP, legal aid, or some other government-funded program). (N.B. There remains debate on the issue and you may wish to speak with your lawyer on the matter.)

There are certain commercial activities that are not covered by PIPEDA. These activities are not subject to the personal information handling rules of the Act. Again, there is doubt about the interpretation of some of these exceptions. For example, it is fairly clear that personal information about employees in the provincial sphere (which includes most employees) is probably not covered by the legislation. However, it is not clear whether personal information about the consultants or contract staff used by the organization to provide its commercial activities is covered. To be prudent, organizations should read these exceptions fairly narrowly until some clear rulings have been made.

(b) Inventory of Personal Information Collected

PIPEDA applies only to personal information. Personal information means information about an identifiable individual. Thus, anonymized information, which cannot be matched to an individual, is no longer personal information. Also, information about a partnership or corporation or other business entity is not normally about an individual. It is unclear whether "individual" includes a person who is dead at the time it is collected, an issue that can be quite significant for some organizations (e.g., health facilities).

The information has to be personal in nature. This would obviously include information about health, personal characteristics and family circumstances. However, some information about the professional activities or capacity of an individual is not personal in nature. For example, the prescribing patterns of a physician have been held not to be personal, but rather to be about their professional capacity (this decision is still under judicial review). Other examples of work product information are letters written by employees in the course of their employment, legal opinions or reports prepared by employees for use by management. In addition, specific exemptions are made for the name, title, business contact information such as telephone numbers, office mailing addresses and, presumably, business email addresses. However, other information even though it has business overtones can still be personal in nature, such as the work hours or income of an individual.

Information does not have to be recorded to be personal. Thus, information requested about an individual but not recorded is still personal information. So are live stream cameras (closed circuit TV) even though no tape or other record is made (and thus privacy principles would apply, e.g., people should know they are under surveillance).

The following are examples of personal information.

Personal Characteristics

- ☐ *Name*
- ☐ *Home contact information*
- ☐ *Identification number (e.g., credit card, social insurance, health, website cookies)*
- ☐ *Insurance benefit coverage*
- ☐ *Identifying features including fingerprints and blood type*
- ☐ *Gender*
- ☐ *Age*
- ☐ *Colour*
- ☐ *Language*
- ☐ *Ethnic or country of origin*
- ☐ *Education or training*
- ☐ *Marital status, sexual history or sexual orientation*
- ☐ *Income*
- ☐ *Social status*
- ☐ *Other: _____*
- ☐ *Other: _____*
- ☐ *Other: _____*

Health

- ☐ *Health history*
- ☐ *Health measurements, samples or examination results*
- ☐ *Health conditions, assessment results, diagnoses*
- ☐ *Health services provided to or received by the person*
- ☐ *Health information collected in the course of providing services*
- ☐ *Prognosis or other opinions formed during assessment and treatment*
- ☐ *Compliance with assessment and treatment*
- ☐ *Reasons for discharge and discharge condition and recommendations*
- ☐ *Bodily donations activities or plans for donations*
- ☐ *Other: _____*
- ☐ *Other: _____*
- ☐ *Other: _____*

Activities and Views

- ☐ *Transaction history with the organization*
- ☐ *Occupation/profession*
- ☐ *Opinions expressed by the person*
- ☐ *Community involvements*
- ☐ *Religion*
- ☐ *Political involvements*
- ☐ *Work hours*
- ☐ *Criminal history*
- ☐ *Disciplinary actions against the individual*
- ☐ *Credit or loan data*
- ☐ *Existence of a dispute with the organization*
- ☐ *Intentions (e.g., to buy goods or services, to change jobs)*
- ☐ *Involvement with organization (e.g., they are a client)*
- ☐ *Letters written to the organization by the person*
- ☐ *Views, evaluations or opinions of the organization about the person*
- ☐ *Other: _____*
- ☐ *Other: _____*

- ☐ *Other: _____*

Many organizations collect personal information primarily about their clients. However, many organizations also collect personal information about third parties as well. A separate part of the Privacy Policy will apply to each category of individuals for whom personal information is collected. Thus, it is important to identify these categories of individuals. These categories of individuals might include the following:

- ☐ *clients*
- ☐ *prospective clients or other members of the general public*
- ☐ *contract staff (non-employees, volunteers, students)*
- ☐ *other: _____*
- ☐ *other: _____*
- ☐ *other: _____*
- ☐ *other: _____*

Step 3 – Collecting Personal Information

(a) Principles of Identifying Purposes and Obtaining Consent

Now that you have an idea of the types of personal information your organization handles and the categories of individuals for which you collect the information, you have to ensure that your information handling practices are consistent with privacy principles. Perhaps the most significant privacy principle is that your organization needs to be able to justify why it needs the information and have authority to collect it. Step 3 deals with this privacy duty.

For any type of personal information collected by your organization, you must identify the following:

- ✓ *the purposes for which you collect the information,*
- ✓ *whether you could limit its collection, and*
- ✓ *by what authority (e.g., consent of the individual, legal exception to the consent requirement) you collect it.*

In other words, you must identify the following:

- ✓ *The **primary purpose** for collecting this information. The primary use of personal information from clients is generally the provision of the good or service sought by them. The purpose must be documented by the organization (which can be done on this form). The purpose must be one which a reasonable person would consider to be appropriate in the circumstances. You have to balance the description of your purposes so that they are not too general as to be meaningless (e.g., "to enable our organization to operate") but not so specific as to be overly detailed or unworkable (e.g., "to enable my assistant to assign a file number when making photocopies of documents on your behalf"). The primary purpose for collecting personal information from non-clients (e.g., members of the public) is not always as obvious and will need to be stated.*
- ✓ *Any **related purposes** for collecting the information. Related purposes support the primary purpose for which the information is gathered (e.g., billing the client if not paid right away, accounting and tax records, follow-up services, etc.). Because some individuals will not immediately think of these purposes, they should be part of the consent process and your Privacy Policy.*
- ✓ *Any other or **secondary purposes** for the information that are likely to arise. Most organizations have secondary uses for the information, such as quality control (a supervisor reviewing the information to ensure that the employee is performing their job well), marketing future special offers to the client, and regulatory accountability (most professionals and organizations are regulated by a self-governing or government agency that has the right to inspect records and investigate complaints). These should be identified in any consent obtained or in the organization's Privacy Policy. Where possible (e.g., marketing future special offers) the client should be given a choice to refuse the secondary use.*
- ✓ *Whether there are steps you can **reasonably take to limit** the collection of personal information. Some information that you currently collect (e.g., social insurance number) may not be necessary to achieve your purposes. If so, you should stop collecting the information. In addition, there may be some information that you do not need to collect every time (e.g., home address and financial information where the client pays at the time of purchase). If so, you should only collect the information if needed. In addition, personal information should only be collected through fair (e.g., without deception) and lawful means.*
- ✓ *How you will **obtain consent, or other legal authority**, for collecting, using or disclosing the information. The intent of the legislation is that personal information will only be collected with the informed consent of the individual, with rare exceptions. To be informed, the individual has to know how the information will be used. Consent can be verbal, written or implied (e.g., where the individual comes to the organization for a particular good or service and the information is obviously necessary to provide the good or service and the individual voluntarily provides the*

information). The form of consent can vary although express consent, particularly in written form, may be preferred when considering the following:

- ✓ *the sensitivity of the information (e.g., health information, financial information),*
- ✓ *the reasonable expectations of the individual, and*
- ✓ *the context (e.g., a written consent is difficult to obtain over the phone).*

Opt out consent forms, requiring action by the individual in order to refuse consent, are frowned upon for sensitive information. Where a person is incapable of consenting (e.g., a child, an incapacitated person), an appropriate substitute can provide the consent (e.g., parent, guardian, spouse, child, power of attorney). You cannot require a client to consent to disclosure of unnecessary information in order to serve another purpose unless that other purpose is specified and legitimate. For example, you cannot require a client to consent to your selling their name and address for marketing purposes if they want to obtain your services; that is tied selling. However, you can require a client to give you reasonable financial information if they are not paying for the good or service at the time because that is reasonably necessary for you to provide them with credit.

Consent can always be withdrawn, in which case future use or disclosure of the information is not permitted if consent is required for it.

The exceptions to obtaining informed consent for collecting personal information include the following:

- ✓ *where collection is clearly in the interests of the individual and consent cannot be obtained in a timely way (e.g., a medical emergency),*
- ✓ *to investigate a breach of a Canadian law or agreement (e.g., a contract) and knowledge or consent would reasonably compromise the investigation,*
- ✓ *for solely journalistic, artistic or literary purposes, or*
- ✓ *publicly available information specified in regulation (e.g., telephone directories, professional directories, statutory registries, court or tribunal records and information provided by the individual to newspapers, magazines and books).*

(b) Primary Purpose and Consent / Other Legal Authority Checklist

PIPEDA applies to the collecting of personal information about any individual, not just clients of the organization. All of these purposes need to be identified. For each category of individuals about whom the organization collects personal information, identify the primary purposes for collecting it on the Checklist document. This will require you to think about the real reason why you collect the information in the first place.

For example, for a health practitioner, the primary purpose for collecting personal information about a client is to provide goods and services for the client. A health practitioner might say: "Our primary purpose for collecting personal information about you is to provide you with health services." The description of that purpose might be: "We collect information about your health history, your physical condition and function, and your social situation in order to help us assess what your needs are, to advise you of your options and then to provide the health care you choose to have." A second primary purpose might be to obtain a baseline of health and social information so that in providing ongoing health services you can identify changes that are occurring.

For most organizations, it is easier to list the primary purposes by category of individuals for which it collects personal information. The purposes are often very different for each category. However, when it comes to related or secondary purposes, the purposes are generally the same for everyone. For that reason, the Checklists documents are divided into two categories. First, you must identify the primary purposes by category of person about whom you collect the information (i.e., clients, general public, contract staff, others). Second, you must identify the related and secondary purposes for all of the personal information you collect.

(c) Related and Secondary Purposes Checklists

For each related or secondary purpose for which the organization collects personal information, complete a separate Checklist in the accompanying document. See section (a) above for a more detailed discussion of related and secondary purposes. Since related and secondary purposes often apply to many or all categories of individuals about whom the organization collects personal information (e.g., quality control), they have not been separated into categories of individuals like the primary purpose section. However, where the related or secondary purpose applies only to some categories (e.g., only clients are invoiced), this is noted under the subheading: "Limitations in Collection".

(d) Principles of Use and Disclosure

Personal information can only be used or disclosed for the purpose for which it was obtained unless:

- ✓ *a further consent is obtained, or*
- ✓ *there is legal authority to use or disclose the information without consent.*

The new use and the consent or other legal authority to use or disclose it should be documented.

Legal authority to use personal information without consent exists in the following circumstances:

- ✓ *where its collection is clearly in the interests of the individual and consent cannot be obtained in a timely way (e.g., a medical emergency),*
  - ✓ *even if not collected for that purpose, there is an emergency that threatens the life, health or security of an individual,*
- ✓ *where its collection was to investigate a breach of a Canadian law or agreement (e.g., a contract) and knowledge or consent would reasonably compromise the investigation,*
  - ✓ *even if not collected for that purpose, the information is reasonably used for the investigation of a breach of law in Canada or elsewhere,*
- ✓ *publicly available information specified in regulation (e.g., telephone directories, professional directories, statutory registries, court records and information provided by the individual to newspapers, magazines and books), or*
- ✓ *specific research situations (obtain legal advice if you believe this narrow ground may apply).*

Legal authority to disclose personal information without consent exists in the following circumstances:

- ✓ *to the organization's lawyer,*
- ✓ *for debt collection purposes,*
- ✓ *to comply with a subpoena, warrant or court order,*
- ✓ *at the request of a government institution for national security, law enforcement or administration,*
- ✓ *at the initiative of the organization, to provide information to a government institution or a specified investigative body relating to law enforcement or national security,*
- ✓ *at the initiative of a specified investigative body relating to law enforcement,*
- ✓ *where there is an emergency that threatens the life, health or security of an individual so long as the person to whom the information relates is then advised in writing right away,*
- ✓ *publicly available information specified in regulation (e.g., telephone directories, professional directories, statutory registries, court records and information provided by the individual to newspapers, magazines and books),*
- ✓ *to an archive,*
- ✓ *20 years after the death of the people to whom the information relates or after 100 years after the record was made,*
- ✓ *specific research situations (obtain legal advice if you believe this narrow ground may apply), or*
- ✓ *where disclosure is required by law.*

There are a number of gaps in the rules permitting the use and disclosure of information without consent. For example, while the organization can disclose personal information to its consultants, it is not clear that the consultants can always share any personal information he or she collects back to the organization. For example, a health practitioner conducting a third party assessment may be permitted to speak to the subject's family to confirm certain information but not be given permission to release that information back to the third party requesting the assessment. For that reason, it may be advisable to anticipate as much as possible any possible uses and disclosures that the organization is likely to need in the original consent process.

Organizations have a duty to take reasonable measures to ensure that any personal information collected is accurate. PIPEDA provides little guidance as to how to achieve this obligation. Suggestions include:

- ✓ *use forms and other standard documents for collecting information that promote the systematic and accurate information,*
- ✓ *where feasible, review the information with the individual at the time of collection,*
- ✓ *in staff training and policies, emphasize the need for information to be accurate and complete,*
- ✓ *if certain information is used regularly, update the information with the individual where possible (although you should not update information if there is no legitimate reason for doing so), and*
- ✓ *welcome requests by the individual to review the accuracy, completeness and currency of personal information about them held by the organization.*

PIPEDA is silent over what is to be done with personal information that has been collected before the Act came into force (on January 1, 2004, for most of the private sector). The former Information and Privacy Commissioner takes the position that any further use or disclosure after that date must be in accordance with the Act (in other words, where consent is required, the organization must go back to the individual for consent). In some circumstances, that approach would be unworkable and there is some doubt as to whether the Information and Privacy Commissioner's interpretation is correct.

Step 4 – Safeguards, Retention and Destruction

(a) Safeguarding Personal Information

Organizations must take appropriate measures to safeguard personal information from unauthorized access, disclosure, use or tampering. The nature of those safeguards will vary depending on the sensitivity of the information and the circumstances. However, those safeguards must include the following components:

- ✓ *physical measures (e.g., restricted access areas, locked filing cabinets),*
- ✓ *organizational measures (e.g., need-to-know and other employee policies, security clearances), and*
- ✓ *technological measures (e.g., passwords, encryption, virus protection, firewalls).*

Organizations need to systematically review all of the places where they may temporarily or permanently hold personal information and assess the adequacy of the safeguards. Almost every organization will find that it needs to make changes to their Privacy Policy.

The federal Information and Privacy Commissioner has published some fact sheets on specific aspects of securing personal information. They are located on the Information and Privacy Commissioner website at: http://www.privcom.gc.ca. Some of the measures suggested there appear to be unworkable for a small organization. The suggestions listed in the accompanying Checklist document may not go quite as far as the Information and Privacy Commissioner would recommend, but may be achievable by a small organization.

(c) Retention and Destruction of Personal Information

The organization is required to have a retention and destruction policy. Retention of personal information should be sufficient for achieving the purpose and to permit the individual to make reasonable inquiries about the personal information of goods/services provided. However, the information should not be kept for a longer period than is reasonably necessary as that provides greater opportunity for the information to be misused or misappropriated. The emphasis by privacy advocates is to shorten the maximum period to as little as possible. The minimum and maximum retention time must be established by policy. While the minimum and maximum times could vary depending on the type of information in issue, for a small organization, it may not be reasonably possible to establish different categories. For organizations that provide one-shot sales, the period would probably be shorter. For organizations that provide professional services, however, regulators often provide rules or guidelines for retention periods (to facilitate on-going services and reports to clients and regulatory scrutiny) that need to be followed. In addition, organizations will wish to keep information for a reasonable time to protect themselves in case of a lawsuit. Thus, a more conservative approach is to set a minimum retention period of six to seven years for professional services (if that is consistent with regulatory requirements) and a maximum of eight to ten years to permit time for destruction of the records.

Because this period is probably longer than some privacy advocates would like, it would be prudent to include this rationale in the related and secondary purposes statements in Step 3, above.

Destruction of personal information must be done in a secure fashion. Typically this involves shredding of paper, deleting of electronic information and the physical destruction of any computer hard drives or electronic data storage containers when they are discarded.

Organizations can have different retention periods for different categories of personal information if desired.

Step 5 – Access, Correction, Complaints and Openness

(a) Access Rights

Individuals have the right, with rare exceptions, to access the personal information about themselves held by the organization and what the organization has done with it. The essential features of these access rights are as follows:

The Request

- ✓ *the organization can require the request to be made in writing (although verbal requests can be answered)*
- ✓ *the organization must assist the requester, if asked to do so*
- ✓ *the organization can charge a minimal cost (e.g., disbursements, but perhaps not all staff time) so long as the individual is notified in advance and indicates that he or she is not withdrawing the request*

Grounds for Refusing a Request

- ✓ *the organization shall provide the member with access to the information and its use and its disclosure to third parties unless one of the following exceptions exist:*
  - ✓ *the information reveals personal information about a third party except where*
    - ✓ *the information about the third party cannot be severed*
    - ✓ *the third party consents or*
    - ✓ *an individual's life, health or safety is threatened*
  - ✓ *the information relates to a warrant, subpoena, disclosure to a government institution or to an investigative body (these provisions are quite complex and legal advice will be needed by the organization)*
  - ✓ *the information is protected by solicitor and client privilege*
  - ✓ *the information would reveal confidential commercial information, unless it can be severed*
  - ✓ *revealing the information could reasonably be expected to threaten the life or security of another individual unless it can be severed*
  - ✓ *the information was collected without consent to investigate a breach of an agreement or law, but then the organization must inform the Information and Privacy Commissioner of the request in writing*
  - ✓ *the information was generated through a formal dispute resolution process (e.g., a professional complaints procedure, ADR)*
- ✓ *access must be provided, despite a ground of refusal (except for the second ground relating to law enforcement) where the individual's life, health or security is threatened*
- ✓ *reasons should be given for a refusal (except for a refusal on the law enforcement ground) and should outline any recourse that is available*
- ✓ *even if the organization refuses the request, it cannot destroy the information until the individual has had a chance to challenge the refusal*

Providing Access

- ✓ *the organization must respond within 30 days (an extension is possible in certain circumstances)*
- ✓ *as stated above, unless a ground of refusal exists, access must be provided*
- ✓ *the organization should confirm the identity of the individual requesting the information before disclosing it*
- ✓ *the organization needs to take reasonable and necessary steps to ensure that the individual requesting it can understand the information (e.g., explain short forms or codes, provide it in an alternative format where the requester has a sensory disability)*
- ✓ *access relates not just to the personal information held, but also how the organization has used and disclosed it (thus, reasonable records should be kept)*

(b) Correction Requests

An individual has the right to request a correction of erroneous personal information held by the organization. If the organization agrees that an error has been made, it must correct the information and, where appropriate, notify any third parties who have received the wrong information of the correction. Where the individual and the organization cannot agree, then the organization must note the disagreement in its file. Again, the organization should notify any third parties who have received the disputed information of the disagreement, where appropriate. This is one of the more ambiguous obligations under PIPEDA. For example, should the correction obliterate the original entry (organizations whose staff are members of regulated professions should probably not obliterate the original entry as the regulatory body may not approve)? Also, does this apply just to factual information, or does it apply to expressions of opinion as well? Finally, when is it not appropriate to advise third parties who received the information?

(c) Complaints System

The organization is required to develop an internal complaints system and make that system along with other, external recourses publicly available. The internal complaints system must have the following features:

- ✓ *a designated individual in the organization (perhaps the Information Officer) to receive, and ensure the prompt* investigation *and response to all complaints*
- ✓ *an easily accessible and simple to use complaints procedure that at a minimum includes*
  - ✓ *acknowledging receipt of the complaint*
  - ✓ *investigating the complaint*
  - ✓ *providing a decision with reasons*
- ✓ *the ability for the organization to respond appropriately to complaints that are justified including making changes to its information handling policies*
- ✓ *notifying the public of external recourses including any regulatory body and the federal Information and Privacy Commissioner*

As seen from both the accompanying Checklist document and the Privacy Policy forms (see sample Forms 2 and 3 below), there are a number of choices to be made in designing the best complaints system for your organization.

The federal Information and Privacy Commissioner has oversight of PIPEDA and acts as an ombudsman. The Commissioner has the following responsibilities:

- ✓ *investigating complaints about an organization's personal information handling practices including entering the organization's premises and summonsing documents and witnesses*
- ✓ *mediating and conciliating such complaints*
- ✓ *auditing the personal information handling practices of an organization*
- ✓ *making a public report of abuses of personal information by an organization*
- ✓ *seeking remedies for a breach of PIPEDA in the Federal Court of Canada*

Once the Commissioner has issued a report, either the complainant or the Commissioner can then apply to the Federal Court of Canada for one or more of the following remedies:

- ✓ *an order for the organization to correct its personal information handling practices*
- ✓ *an order for the organization to publish a notice of corrective action*
- ✓ *an award of damages for any humiliation of the complainant*

(d) Openness

The organization must make its personal information handling Privacy Policy available to the public. Individuals must be able to obtain this Privacy Policy without unreasonable effort. The Privacy Policy must be generally understandable. The accompanying Checklist document and the Privacy Policy (samples are found at Forms 2 and 3, below) is an attempt to provide the tools for your organization to prepare such a document.

A large organization might have three separate documents:

- ✓ *a brochure summarizing the organization's Privacy Policy document*
- ✓ *a comprehensive Privacy Policy document*
- ✓ *an internal operational guide to assist staff in implementing the Privacy Policy document.*

A smaller organization might simply use one Privacy Policy document.

Step 6 – Implementing Your Privacy Plan

Implementing your Privacy Policy will have two stages. The first stage will be to complete your review of how you handle personal information and to prepare and roll out your Privacy Policy. The second stage is to periodically monitor, review and update your Privacy Policy. During your first year, the monitoring, review and updating should be fairly frequent as issues arise. However, after that, you must regularly review things. The Information and Privacy Commissioner has criticized organizations for having a policy in writing that does not reflect what is actually happening. At a minimum, a specific date should be set each year (e.g., July) to monitor, review and update the Privacy Policy. That annual review should be documented in case the Information and Privacy Commissioner comes calling.

Form 1 Health Consent Form

NOTE TO CLIENT *We want your informed consent. This means that we want you to understand the services we hope to provide to you, the cost involved, and what we do with personal information we obtain about you. If you have a question on any of this, please ask.*

CONSENT FOR TREATMENT
[Insert your usual consent for treatment provisions here.]

CONSENT FOR THE COST OF OUR SERVICES
[Insert your usual financial provisions here.]

CONSENT FOR PERSONAL INFORMATION
I understand that to provide me with *[name of health profession]* goods and services, *[name of your organization]* will collect some personal information about me (e.g.*, [set out some common examples like home telephone number, address]*).

I have reviewed the *[name of organization]*'s Privacy Policy about the collection, use and disclosure of personal information, steps taken to protect the information and my right to review my personal information. I understand how the Privacy Policy applies to me. I have been given a chance to ask any questions I have about the Privacy Policies and they have been answered to my satisfaction.

I understand that only if I check off the following boxes will I receive the following: *[insert opt-in clauses where opt-out consent would not be appropriate]*

- ❑ I would like to receive notice when it is time to review whether I need new goods or services.
- ❑ I would like to receive newsletters and other informational mailings from *[name of organization].*
- ❑ I would like to receive notice of promotions and special offers from *[name of organization.]*
- ❑ I would like to receive newsletters and other informational mailings and notice of promotions and special offers from other organizations that *[name of organization]* thinks might be of interest to me.

I understand that, as explained in the Policies and Procedures for Personal Information, there are some rare exceptions to these commitments.

I agree to *[name of organization]* collecting, using and disclosing personal information about me as set out above and in the *[name of organization]*'s Privacy Policy.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

NOTES MADE BY *[name of organization]*
_____
_____
_____

Form 2 Privacy Policy – Generic Form

Privacy of personal information is an important principle to *[name of organization]*. We are committed to collecting, using and disclosing personal information responsibly and only to the extent necessary for the goods and services we provide. We also try to be open and transparent as to how we handle personal information. This document describes our privacy policies.

WHAT IS PERSONAL INFORMATION?
Personal information is information about an identifiable individual. Personal information includes information that relates to their personal characteristics (e.g., gender, age, income, home address or phone number, ethnic background, family status), their health (e.g., health history, health conditions, health services received by them) or their activities and views (e.g., religion, politics, opinions expressed by an individual, an opinion or evaluation of an individual). Personal information is to be contrasted with business information (e.g., an individual's business address and telephone number), which is not protected by privacy legislation.

WHO WE ARE
Our organization, *[insert name],* includes *[describe].* We use a number of consultants and agencies that may, in the course of their duties, have limited access to personal information we hold. These include *[list them by category or name]*. We restrict their access to any personal information we hold as much as is reasonably possible. We also have their assurance that they follow appropriate privacy principles.

WE COLLECT PERSONAL INFORMATION: PRIMARY PURPOSES
Like all *[name nature of your business]*, we collect, use and disclose personal information in order to serve our clients.

For our clients, the primary purposes for collecting personal information are as follows: *[insert purpose identified by you in Part 3(b) of the checklist]*. Examples of the type of personal information we collect for those purposes include the following: *[insert information compiled by you in Part 3(b) of the checklist]*. *[If you collect personal information about clients without their consent, provide a brief description of when you might do this if at all possible.*]

For members of the general public, our primary purposes for collecting personal information are as follows: *[insert purpose identified by you in Part 3(b) of the checklist]*. Examples of the type of personal information we collect for those purposes include the following: *[insert information compiled by you in Part 3(b) of the checklist]*. *[If you collect personal information about members of the general public without their consent, provide a brief description of when you might do this if at all possible.]*

For contract staff (e.g, temporary workers *[set out other examples])*, our primary purposes for collecting personal information are as follows: *[insert purpose identified by you in Part 3(b) of the checklist]*. Examples of the type of personal information we collect for those purposes include the following: *[insert information compiled by you in Part 3(b) of the checklist]*. *[If you collect personal information about contract staff without their express consent, provide a brief description of when you might do this if at all possible.]*

When we investigate, audit or assess a person for someone else (e.g., *[set out examples such as for a legal investigation, financial audit, medical assessment])*, our primary purposes for collecting personal information are as follows: *[insert purpose identified by you in Part 3(b) of the checklist]*. Examples of the type of personal information we collect for those purposes include the following: *[insert information compiled by you in Part 3(b) of the checklist]*. *[If you collect personal information*

about third parties without their express consent, provide a brief description of when you might do this if at all possible.]

For *[insert other categories, if any]*, our primary purposes for collecting personal information are as follows: *[insert purpose identified by you in Part 3(b) of the checklist]*. Examples of the type of personal information we collect for those purposes include the following: *[insert information compiled by you in Part 3(b) of the checklist]*. *[If you collect personal information about [insert other categories, if any] without their consent, provide a brief description of when you might do this if at all possible.]*

WE COLLECT PERSONAL INFORMATION: RELATED AND SECONDARY PURPOSES

Like most organizations, we also collect, use and disclose information for purposes related to or secondary to our primary purposes. The most common examples of our related and secondary purposes are as follows:

- *[Set out each related or secondary purpose that relates to your organization as identified in Part 3(c) of the checklist. Briefly describe the purpose, identify any additional personal information collected just for that purpose, any limitations in that collection and the authority for this purpose. See Form 3 for a precedent for this section.]*

You can choose not to be part of some of these related or secondary purposes (e.g., by declining special offers or promotions, by paying for your services in advance). We do not, however, have much choice about some of these related or secondary purposes (e.g., external regulation).

PROTECTING PERSONAL INFORMATION

We understand the importance of protecting personal information. For that reason, we have taken the following steps *[change the following points as necessary as set out in part 4(b) of the checklist; see Form 3 for an example]*:

- Paper information is either under supervision or secured in a locked or restricted area.
- Electronic hardware is either under supervision or secured in a locked or restricted area at all times. In addition, passwords are used on computers. All of our cell phones are digital, which signals are more difficult to intercept.
- Paper information is transmitted through sealed, addressed envelopes or boxes by reputable companies.
- Electronic information is transmitted either through a direct line or is anonymized or encrypted.
- Staff are trained to collect, use and disclose personal information only as necessary to fulfill their duties and in accordance with our privacy policy.
- External consultants and agencies with access to personal information must enter into privacy agreements with us.

RETENTION AND DESTRUCTION OF PERSONAL INFORMATION

We need to retain personal information for some time to ensure that we can answer any questions you might have about the services provided and for our own accountability to external regulatory bodies. However, we do not want to keep personal information too long in order to protect your privacy. *[Summarize your retention and destruction policies here as set out in Part 4(c) of the checklist. See Form3 for an example.]* We keep our client files for about ____ years. Our client and contact directories are much more difficult to systematically destroy, so we remove such information when we can if it does not appear that we will be contacting you again. However, if you ask, we will remove such contact information right away. We keep any personal information relating to our general correspondence with people who are not our clients, newsletters, seminars and marketing activities for about ____ months after the newsletter, seminar or marketing activity is over.

We destroy paper files containing personal information by shredding. We destroy electronic information by deleting it and, when the hardware is discarded, we ensure that the hard drive is physically destroyed. Alternatively, we may send some or all of the client file to our client.

YOU CAN LOOK AT YOUR INFORMATION

With only a few exceptions, you have the right to see what personal information we hold about you. Often all you have to do is ask. We can help you identify what records we might have about you. We will also try to help you understand any information you do not understand (e.g., short forms, technical language, etc.). We will need to confirm your identity, if we do not know you, before providing you with this access. We reserve the right to charge a nominal fee for such requests.

If there is a problem, we may ask you to put your request in writing. If we cannot give you access, we will tell you within 30 days if at all possible and tell you the reason, as best we can, as to why we cannot give you access.

If you believe there is a mistake in the information, you have the right to ask for it to be corrected. This applies to factual information and not to any professional opinions we may have formed. We may ask you to provide documentation that our files are wrong. Where we agree that we made a mistake, we will make the correction and notify anyone to whom we sent this information. If we do not agree that we have made a mistake, we will still agree to include in our file a brief statement from you on the point and we will forward that statement to anyone else who received the earlier information.

DO YOU HAVE A CONCERN?

Our Information Officer, *[insert name],* can be reached at *[insert contact information]* to address any questions or concerns you might have.

If you wish to make a formal complaint about our privacy practices, you may make it in writing to our Information Officer. S/he will acknowledge receipt of your complaint, ensure that it is investigated promptly and that you are provided with a formal decision and reasons in writing.

For more general inquiries, the Information and Privacy Commissioner of Canada oversees the administration of the privacy legislation in the private sector. The Commissioner also acts as a kind of ombudsman for privacy disputes. The Information and Privacy Commissioner can be reached at:

112 KENT STREET | OTTAWA, ONTARIO | K1A 1H3
PHONE (613) 995-8210 | **TOLL-FREE** 1-800-282-1376 | **FAX** (613) 947-6850 | **TTY** (613) 992-9190
www.privcom.gc.ca

Form 3 Privacy Policy – Health Practitioner Sample Form

Privacy of personal information is an important principle to the Green Sombretherapy Clinic. We are committed to collecting, using and disclosing personal information responsibly and only to the extent necessary for the goods and services we provide. We also try to be open and transparent as to how we handle personal information. This document describes our privacy policies.

WHAT IS PERSONAL INFORMATION?
Personal information is information about an identifiable individual. Personal information includes information that relates to their personal characteristics (e.g., gender, age, income, home address or phone number, ethnic background, family status), their health (e.g., health history, health conditions, health services received by them) or their activities and views (e.g., religion, politics, opinions expressed by an individual, an opinion or evaluation of an individual). Personal information is to be contrasted with business information (e.g., an individual's business address and telephone number), which is not protected by privacy legislation.

WHO WE ARE
Our organization, Green Sombretherapy Clinic*,* includes at the time of writing three Sombretherapists and four support staff*.* We use a number of consultants and agencies that may, in the course of their duties, have limited access to personal information we hold. These include computer consultants, office security and maintenance, bookkeepers and accountants, temporary workers to cover holidays, credit card companies, website managers, cleaners and lawyers. We restrict their access to any personal information we hold as much as is reasonably possible. We also have their assurance that they follow appropriate privacy principles.

WE COLLECT PERSONAL INFORMATION: PRIMARY PURPOSES
About Clients
Like all sombretherapists, we collect, use and disclose personal information in order to serve our clients. For our clients, the primary purpose for collecting personal information is to provide sombretherapy treatment. For example, we collect information about a client's health history, including their family history, physical condition and function and social situation in order to help us assess what their health needs are, to advise them of their options and then to provide the health care they choose to have. A second primary purpose is to obtain a baseline of health and social information so that in providing ongoing health services we can identify changes that are occurring over time. It would be rare for us to collect such information without the client's express consent, but this might occur in an emergency (e.g., the client is unconscious) or where we believe the client would consent if asked and it is impractical to obtain consent (e.g., a family member passing a message on from our client and we have no reason to believe that the message is not genuine).

About Members of the General Public
For members of the general public, our primary purposes for collecting personal information are to provide notice of special events (e.g., a seminar or conference) or to make them aware of sombretherapy services in general or our clinic in particular. For example, while we try to use work contact information where possible, we might collect home addresses, fax numbers and email addresses. We try to obtain consent before using any such personal information, but where this is not, for any reason, possible, we will upon request immediately remove any personal information from our distribution list.

On our website we only collect, with the exception of cookies, the personal information you provide and only use that information for the purpose you gave it to us (e.g., to respond to your email

message, to register for a course, to subscribe to our newsletter). Cookies are only used to help you navigate our website and are not used to monitor you.

About Contract Staff, Volunteers and Students

For people who are contracted to do work for us (e.g., temporary workers), our primary purpose for collecting personal information is to ensure we can contact them in the future (e.g., for new assignments) and for necessary work-related communication (e.g., sending out paycheques, year-end tax receipts). Examples of the type of personal information we collect for those purposes include home addresses and telephone numbers. It is rare for us to collect such information without prior consent, but it might happen in the case of a health emergency (e.g., a SARS outbreak) or to investigate a possible breach of law (e.g., if a theft were to occur in the clinic). If contract staff, volunteers or students wish a letter of reference or an evaluation, we will collect information about their work related performance and provide a report as authorized by them.

WE COLLECT PERSONAL INFORMATION: RELATED AND SECONDARY PURPOSES

Like most organizations, we also collect, use and disclose information for purposes related to or secondary to our primary purposes. The most common examples of our related and secondary purposes are as follows:

- To invoice clients for goods or services that were not paid for at the time, to process credit card payments or to collect unpaid accounts.
- To advise clients that their product or service should be reviewed (e.g., to ensure a product is still functioning properly and appropriate for their then current needs and to consider modifications or replacement).
- To advise clients and others of special events or opportunities (e.g., a seminar, development of a new service, arrival of a new product) that we have available.
- Our clinic reviews client and other files for the purpose of ensuring that we provide high quality services, including assessing the performance of our staff. In addition, external consultants (e.g., auditors, lawyers, practice consultants, voluntary accreditation programs) may on our behalf do audits and continuing quality improvement reviews of our Clinic, including reviewing client files and interviewing our staff.
- Sombretherapists are regulated by the College of Sombretherapists of Ontario who may inspect our records and interview our staff as a part of their regulatory activities in the public interest. In addition, as professionals, we will report serious misconduct, incompetence or incapacity of other practitioners, whether they belong to other organizations or our own. Also, our organization believes that it should report information suggesting serious illegal behaviour to the authorities. External regulators have their own strict privacy obligations. Sometimes these reports include personal information about our clients, or other individuals, to support the concern (e.g., improper services). Also, like all organizations, various government agencies (e.g., Canada Customs and Revenue Agency, Information and Privacy Commissioner, Human Rights Commission, etc.) have the authority to review our files and interview our staff as a part of their mandates. In these circumstances, we may consult with professionals (e.g., lawyers, accountants) who will investigate the matter and report back to us.
- The cost of some goods/services provided by the organization to clients is paid for by third parties (e.g., OHIP, WSIB, private insurance, Assistive Devices Program). These third-party payers often have your consent or legislative authority to direct us to collect and disclose to them certain information in order to demonstrate client entitlement to this funding.
- Clients or other individuals we deal with may have questions about our goods or services after they have been received. We also provide ongoing services for many of our clients over a period of months or years for which our previous records are helpful. We retain our client

information for a minimum of ten years after the last contact to enable us to respond to those questions and provide these services (our regulatory College also requires us to retain our client records).

- If the Green Sombretherapy Clinic or its assets were to be sold, the purchaser would want to conduct a "due diligence" review of the Clinic's records to ensure that it is a viable business that has been honestly portrayed to the purchaser. This due diligence may involve some review of our accounting and service files. The purchaser would not be able to remove or record personal information. Before being provided access to the files, the purchaser must provide a written promise to keep all personal information confidential. Only reputable purchasers who have already agreed to buy the organization's business or its assets would be provided access to personal information, and only for the purpose of completing their due diligence search prior to closing the purchase.

You can choose not to be part of some of these related or secondary purposes (e.g., by declining to receive notice of special events or opportunities, by paying for your services in advance). We do not, however, have much choice about some of these related or secondary purposes (e.g., external regulation).

PROTECTING PERSONAL INFORMATION

We understand the importance of protecting personal information. For that reason, we have taken the following steps*:*

- Paper information is either under supervision or secured in a locked or restricted area.
- Electronic hardware is either under supervision or secured in a locked or restricted area at all times. In addition, passwords are used on computers. All of our cell phones are digital, which signals are more difficult to intercept.
- Paper information is transmitted through sealed, addressed envelopes or boxes by reputable companies.
- Electronic information is transmitted either through a direct line or is anonymized or encrypted.
- Staff are trained to collect, use and disclose personal information only as necessary to fulfill their duties and in accordance with our privacy policy.
- External consultants and agencies with access to personal information must enter into privacy agreements with us.

RETENTION AND DESTRUCTION OF PERSONAL INFORMATION

We need to retain personal information for some time to ensure that we can answer any questions you might have about the services provided and for our own accountability to external regulatory bodies. However, we do not want to keep personal information too long in order to protect your privacy.

We keep our client files for about ten years. Our client and contact directories are much more difficult to systematically destroy, so we remove such information when we can if it does not appear that we will be contacting you again. However, if you ask, we will remove such contact information right away. We keep any personal information relating to our general correspondence (i.e., with people who are not clients) newsletters, seminars and marketing activities for about six months after the newsletter ceases publication or a seminar or marketing activity is over.

We destroy paper files containing personal information by shredding. We destroy electronic information by deleting it and, when the hardware is discarded, we ensure that the hard drive is physically destroyed. Alternatively, we may send some or all of the client file to our client.

YOU CAN LOOK AT YOUR INFORMATION

With only a few exceptions, you have the right to see what personal information we hold about you. Often all you have to do is ask. We can help you identify what records we might have about you. We will also try to help you understand any information you do not understand (e.g., short forms, technical language, etc.). We will need to confirm your identity, if we do not know you, before providing you with this access. We reserve the right to charge a nominal fee for such requests.

If there is a problem we may ask you to put your request in writing. If we cannot give you access, we will tell you within 30 days if at all possible and tell you the reason, as best we can, as to why we cannot give you access.

If you believe there is a mistake in the information, you have the right to ask for it to be corrected. This applies to factual information and not to any professional opinions we may have formed. We may ask you to provide documentation that our files are wrong. Where we agree that we made a mistake, we will make the correction and notify anyone to whom we sent this information. If we do not agree that we have made a mistake, we will still agree to include in our file a brief statement from you on the point and we will forward that statement to anyone else who received the earlier information.

DO YOU HAVE A QUESTION?

Our Information Officer, Rose Green*,* can be reached at:

12 Blue Bay Rd. | Pinkville, ON | M9M 9M9
PHONE (613) 555-2121

She will attempt to answer any questions or concerns you might have.

If you wish to make a formal complaint about our privacy practices, you may make it in writing to our Information Officer. She will acknowledge receipt of your complaint, ensure that it is investigated promptly and that you are provided with a formal decision and reasons in writing.

If you have a concern about the professionalism or competence of our services or the mental or physical capacity of any of our professional staff we would ask you to discuss those concerns with us. However, if we cannot satisfy your concerns, you are entitled to complain to our regulatory body:

COLLEGE OF SOMBRETHERAPISTS OF ONTARIO
[Address, telephone, fax and email, website information]

This policy is made under the *Personal Information Protection and Electronic Documents Act*. That is a complex Act and provides some additional exceptions to the privacy principles that are too detailed to set out here. There are some rare exceptions to the commitments set out above.

For more general inquiries, the Information and Privacy Commissioner of Canada oversees the administration of the privacy legislation in the private sector. The Commissioner also acts as a kind of ombudsman for privacy disputes. The Information and Privacy Commissioner can be reached at:

112 KENT STREET | OTTAWA, ONTARIO | K1A 1H3
PHONE (613) 995-8210 | **TOLL-FREE** 1-800-282-1376 | **FAX** (613) 947-6850 | **TTY** (613) 992-9190
www.privcom.gc.ca