PERSONAL INFORMATION PROTECTION
and ELECTRONIC DOCUMENTS ACT

On January 1, 2004, the Federal ***Personal Information Protection and Electronic Documents Act***, S.C. 2000, c. 5, came into effect for all organizations that collect, use or disclose personal information in the course of commercial activities. An "organization" is defined to include an association, a partnership, a person and a trade union. Thus, an organization could include a firm of practitioners who operate as a partnership, or through a limited company, or even one practitioner who operates by herself.

APPLICATION

The application provision in the Act (s. 4) states that it applies to every organization in respect of personal information that the organization collects, uses, or discloses in the course of commercial activities. Thus, if a firm of occupational therapists holds itself out and provides services to the public for remuneration, i.e., engages in commercial activity, it is the firm that is the "organization" in that case. Conversely, if it is a sole practitioner, it is the sole practitioner which is the "organization" in that case.

The legislation makes no distinction between large and small organizations. Thus, at least from a strictly legal point of view, the legislation applies equally to a one-person "organization" as it does to a very large business corporation. Equally, the legislation applies to the small occupational therapist practitioner.

PERSONAL INFORMATION

The Act contains a very broad definition of personal information - it is any information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization. It should be noted that the information must relate to a natural human being, as opposed to a legal entity, such as a corporation. It would seem that it

need not precisely identify the individual to be considered to be personal information, so long as the individual can be identified through some other means which is reasonable available. For example, if there is a distinguishing number or code which can somehow be readily cross-referenced to the actual individual, that would then be considered to be personal information. On the other hand, if the information has been rendered truly anonymous, then it would no longer be considered personal information for purposes of the Act.

It is also to be noted that the definition excludes the name, title, business address or telephone number of an employee of an organization. At this stage, it is not clear whether other business or employment information would be included from personal information.

THE TEN PRINCIPLES

The Act contains, in Schedule I, a list of ten guiding principles and related explanation and rules. Readers are referred to the actual legislation and advised to read the full Schedule 1. What follows herein is the main principle (in italics) and a statement of the practical implications (in regular text)

- *4.1 Principle 1-Accountability*

  An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

  The organization should appoint an individual (or individuals) to be responsible for your organization's compliance; protect all personal information held by your organization or transferred to third party for processing; and develop and implement personal information policies and practices.

- *4.2 Principle 2- Identifying Purposes*

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

The organization must identify the reasons for collecting personal information before or at the time of collection. Before or when any personal information is collected, identify why it is needed and how it will be used; document why the information is collected; inform the individual from whom the information is collected why it is needed; identify any new purpose for the information and obtain the individual's consent before using it.

- *4.3 Principle 3- Consent*

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

The organization must inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data; obtain the individual's consent before or at the time of collection, as well as when a new use is identified.

- *4.4 Principle 4- Limiting Collection*

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

The organization can not collect personal information indiscriminately and can not deceive or mislead individuals about the reasons for collecting personal information.

- *4.5 Principle 5- Limiting Use, Disclosure, Retention*

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

The organization may use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act; keep personal information only as long as necessary to satisfy the purposes; put guidelines and procedures in place for retaining and destroying personal information; keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress; destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

- *4.6 Principle 6- Accuracy*

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

The organization must minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

- *4.7 Principle 7- Safeguards*

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

The organization must protect personal information against loss or theft; safeguard the information from unauthorized access, disclosure, copying, use or modification

- *4.8 Principle 8-Openness*

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

The organization must inform its customers, clients and employees that it has policies and practices for the management of personal information; make these policies and practices understandable and easily available.

- *4.9 Principle 9- Individual Access*

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

When requested, the organization must inform individuals if it has any personal information about them; explain how it is or has been used and provide a list of any organizations to which it has been disclosed; give individuals access to their information; correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient; provide a copy of the information requested, or reasons for not providing access, where doing so would provide information about a third party that cannot be severed; an organization should note any disagreement on the file and advise third parties where appropriate.

- *4.10 Principle 10-Challenging Compliance*

  An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

> Develop simple and easily accessible complaint procedures; inform complainants of avenues or recourse. These include your organization's own complaint procedures, those of industry associations, regulatory bodies and the Privacy Commissioner of Canada; investigate all complaints received; take appropriate measures to correct information handling practices and policies.

It should be emphasized that further provisions are contained in the actual Schedule and it is strongly recommended that you review the full text of the legislation and the Schedule. This can be found by accessing the Federal Privacy Commissioner's website, which is at "www.privcom.gc.ca".

COMPLAINT PROCESS and REMEDIES

An individual may make a written complaint to the Privacy Commissioner, who may then investigate the complaint. The Commissioner has broad powers, including power to compel evidence, administer rules, accept any evidence and even enter a premises. The ultimate remedies include ordering the organization to correct its practices in order to comply with the provisions of the Act, order the organization to publish a notice of action to take to correct its practices, and/or award damages, including damages for humiliation the complainant may have suffered. As well, the Commissioner may perform audits to ensure compliance with the provisions of the Act.

COMPLIANCE PLAN

Some items which should be implemented are as follows (and by no means is this suggested to be exhaustive):

- Educate and train all members of the firm about the new legislation. This will take some time. The best starting place would be the website referred to above (www.privcom.gc.ca). In particular, following the link "New! e-kit", under the Resource Centre heading, will lead to an article entitled "Information on PIPEDA for Health Care Sector Organizations". This material is done by way of questions and answers (question 19 is attached as Appendix "A").
- Appoint an Information Officer. This should be a reasonably senior person within an organization. In a one-person firm, it would be that person.

  The Information Officer would have the responsibility to develop and implement the organization's compliance with the legislative requirements.

- Review/Audit the personal information that the organization currently collects, uses and discloses.

- Develop the organization's policies and practices for compliance with the PIPEDA principles. This material should contain procedures regarding the storage and safeguarding of personal information, and provide for a process for individuals to access and correct personal information. It should contain a retention policy, a training policy and a complaints process. One part of the firm's overall policy should be a privacy policy document to explain and communicate the firm's policy to the public and its customers/patients. A very basic privacy policy is attached as Appendix "B" to these materials.