Privacy - Your Responsibilities under the Act

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 privacy principles. A good understanding of Canada' Personal Information Protection and Electronic Documents Act (PIPEDA) will help offset privacy issues. For further information visit the website: www.privcom.gc.ca.

2. Identifying Purposes: The purposes for which personal information is collected shall be identified by the broker/organization at or before the time the information is collected. Define your purpose for collecting data as clearly and narrowly as possible so the individual can understand how the information will be used or disclosed.

3. Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate. Consent is only meaningful if the individuals understand how their information will be used.

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. Only obtain the information necessary for the service or product being provided.

5. Limiting Use, Disclosure, and 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 the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes. Conduct regular reviews to help determine whether information is still required.

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. One way to determine if information needs to be updated is to ask whether the use or disclosure of out of date or incomplete information would harm the individual.

7. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Keep sensitive information files in a secure area or computer system and limit access to individuals on a "need-to-know" basis only.

8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. Information about policies and practices may be made available in person, in writing, by telephone, in publications or on an organization's website.

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. Keep personal information about individuals in one place to make retrieval easier or record where all such information can be found. Never disclose personal information unless you are sure of the identity of the requestor and that person's right to access.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance. How well you handle an individual's complaint may help preserve or restore the individual's confidence in an organization.