

A COMMENTARY ON LEGAL ISSUES AFFECTING PROFESSIONAL REGULATION

Safeguarding Personal Information

One of the more significant requirements of the new privacy legislation is the need to safeguard personal information. The *Personal Information Protection and Electronic Documents Act* (PIPEDA), which takes effect on January 1, 2004, requires organizations to secure personal information from unauthorized access, disclosure, use or tampering.

These requirements will be mandatory for most members of regulated professions. Regulators have an important role to educate their members of the new requirements. Regulators cannot afford to let their own information handling practices fall below the standard expected of their members.

Safeguarding of client information has always been an important duty of members. However, with some exceptions (e.g., public hospitals, some government departments), the level of diligence is not what the federal Information and Privacy Commissioner would expect. Private offices are, perhaps, somewhat complacent and could benefit from a systematic review of their practices. The impending arrival of PIPEDA is a good opportunity for regulators to remind their members of their obligations.

Overview

Safeguarding personal and other confidential information will require 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).

Location of Paper Information

Practitioners need to consider one or more of the following options for safeguarding information:

- restricting working areas to staff only,
- ensuring that non-staff are supervised at all times when in the working area,
- obtaining written assurances of privacy and confidentiality from non-staff (e.g., cleaners) with unsupervised physical, and
- locking confidential information away when the staff person working on it is not present, (e.g., breaks and overnight).

Staff who remove information from the office or take work home need to ensure that

FOR MORE INFORMATION

This newsletter is published by Steinecke Maciura LeBlanc, a law firm practising in the field of professional regulation. If you are not receiving a copy and would like one, please contact:

Richard Steinecke
Steinecke Maciura LeBlanc
Law Chambers, University Centre
Suite 2000, 393 University Avenue
Toronto, Ontario M5G 1E6

Telephone: 416-626-6897 Facsimile: 416-593-7867
E-Mail: rsteinecke@sympatico.ca

Grey Areas is also available on our website: www.sml-law.com. Some back issues are also available.

WANT TO REPRINT AN ARTICLE

A number of readers have asked to reprint articles in their own newsletters. Our policy is that readers may reprint an article as long as credit is given to both the newsletter and the firm. Please send us a copy of the issue of the newsletter which contains a reprint from Grey Areas.

there is no access during transit (e.g., either kept in direct physical possession or kept in a locked space). Given the number of people who come in and out of our homes, there probably needs to be a locked room or cabinet for information kept there.

Location of Electronic Information

Access to the hardware housing electronic information (e.g., computers, laptops, tapes and disks) should probably have protections similar to that of paper information. In addition, both log-on and screen saver passwords should be used. Every computer needs to have both firewall and anti-virus protection. Computers used for work purposes at home need a similar level of protection. Other family members should not have access to work-related information, perhaps through a separate user password.

Transfer of Paper Information

Practitioners need to consider one or more of the following options for sending paper documents:

- in sealed envelope, marked private and confidential, sent by Canada Post or reputable courier,
- in sealed envelope, marked private and confidential, delivered by staff, or
- in sealed envelope to be picked up by person who asks for it by name of recipient (kept out of sight in reception area until picked up).

Transfer of Electronic Information

Safeguarding electronic information transfers will probably be the greatest challenge for most organizations. The Information and Privacy Commissioner has indicated that regular email is not an acceptable means for transferring sensitive

personal information. However, the use of unencrypted email has become so convenient that there is a very strong temptation to ignore this expectation. Regulators will have to be vigorous in their education of members that they should use one of the following options:

- with the consent of the person to whom the personal information relates (e.g., the client requests email communication) (N.B., the recipient is not necessarily the person to whom the personal information relates),
- where the message is anonymized, or
- encryption is used

For smaller organizations, finding an encryption program that is easy to use is a problem. Electronic signature protection is probably not sufficient. For all practical purposes, either the recipient has to use the same program or a secure website access program is required.

Even faxes can go astray. Fax number input errors and faxing confidential documents to a machine in an unsecured area are recurring problems. Practitioners will want to consider the following measures.

- securely locating your incoming fax machine.
- use a cover sheet identifying the recipient with a privacy clause on it and one of the following safeguards:
 - o fax number has been approved by the recipient,
 - o the recipient has advised that the fax machine is securely located,
 - o in the context, the privacy of the recipient fax machine can reasonably be inferred (e.g., the fax is to a legal, accounting or health care office), or

- the recipient has a Privacy Policy.

Websites require special security measures if they collect or contain personal information (e.g., an appropriate website cookie policy must be in place).

Staff Safeguards

Practitioners should ensure that staff (including temporary workers) are trained in the following:

- the importance of the privacy of personal information.
- access to personal information within the organization is on a need-to-know basis.
- the organization's Privacy Policy on information handling, including obtaining consent before collecting personal information, only using information for the purpose for which the consent was provided and the name of the Privacy Officer for the organization.
- sensitivity in collecting or using personal information verbally where others might overhear.
- when providing copies of personal information internally or externally, to remove or mask unnecessary personal information.
- to recognize and avoid being "pumped" for information.
- to ensure that any personal information is not accidentally discarded in the regular garbage or blue box disposal system, but rather is shredded.
- to avoid discussing personal information in public places (e.g., elevators, restaurants, washrooms, public transit).
- that a breach of the organization's policies will result in discipline up to and including dismissal.

Consultants and Contractors

Practitioners need to review their privacy and security agreements with all consultants and contractors who have access to personal or other confidential information. A documented assurance from each of them will state that they will not access personal information except as required in the course of their duties and shall not be collected, used or disclosed for any other purpose without consent. The following consultants and contractors might be involved.

- temporary workers
- cleaners
- information technology
- marketers
- legal
- bookkeeping and accounting
- file storage
- credit card companies
- website manager
- office security
- building maintenance
- landlord

Regulators should use the advent of PIPEDA as a reason to remind their members to review and update their own practices.

See our website (www.sml-law.com) for additional information about privacy issues, including our seminars designed to help practitioners develop their own privacy policy.