

GUIDE TO GOOD PRIVACY PRACTICES

Introduction:

The purpose of this guide is to assist public bodies in meeting their privacy responsibilities under Part III (Protection of Privacy) of the *Freedom of Information and Protection of Privacy Act* (the Act). This guide is intended to supplement the Act by giving general staff a set of principles upon which to base day-to-day decisions about managing personal information in their program area. The guide's intended audience is public body managers. Managers may then utilize the guide, as they deem desirable, for the benefit of front line staff.

Privacy principles are not absolute. In administering the Act, public bodies must balance the public's right to hold public bodies accountable and the protection of personal privacy. In some cases, a balance must be struck between privacy rights and the public interest. In others, legislation requires the collection or disclosure of personal information that must take precedence over privacy principles (i.e. the *Family and Child Service Act* requires disclosure of evidence of suspected child abuse). Public bodies must consider all of these issues when making decisions about managing personal information.

The Act sets certain *minimum* requirements for privacy that public bodies must follow. Instead of limiting privacy protection only to these standards, public bodies should adopt the *maximum* level of privacy protection that they can afford within their legal and operational requirements.

The guide includes a list and description of privacy principles as well as some information about the powers of the Commissioner of Information and Privacy with respect to privacy. Adopting the practices and principles of this guide will help public bodies to increase awareness about privacy implications and reduce the chance of being censured publicly by the Commissioner.

PRIVACY PRINCIPLES

1. Limitations on the Collection of Personal Information

Public bodies should collect personal information only when it is essential for program delivery. Public bodies should review current collection practices on a regular basis to determine if all of the information currently collected is still needed. They should also be prepared to justify why particular information is necessary. The best example of non-essential information sometimes collected by public bodies is the Social Insurance Number (SIN). The SIN was introduced solely for the purposes of taxation and social security administered by the federal government. Nevertheless, provincial public bodies sometimes collect it for purposes of identification. When the SIN is collected and used for a number of purposes, however, there is a greater potential for an invasion of privacy. It creates opportunities for some individuals to undermine the personal privacy of others by creating a personal profile from a wide variety of information linked to that

number. Therefore, public bodies should collect and use the SIN only for purposes authorized by legislation. If you are uncertain about whether a use of the SIN is authorized by legislation, contact your Director/Manager of Information and Privacy (DMIP) or FOI Coordinator.

Public bodies should periodically review their programs to determine the minimum personal information that is essential for their operational requirements, and should not collect information that does not meet this criteria. In cases where individuals are reluctant to disclose certain personal information that is not essential, public bodies should not deny service to them. If individuals object to disclosing certain personal information, public bodies should make their best effort to accommodate them. Explain why it is necessary to collect the information that is essential and allow them to withhold information that is not essential.

2. Individuals and the Protection of their Privacy Rights

Two of the key principles underlying the Act are that individuals own their own information and have a general right to privacy. While this does not mean that individuals have full control over records containing their information, public bodies should treat them as stakeholders in the collection, use and disclosure of their own personal information. Public bodies can help to achieve this goal by incorporating the following principles into their records management practices:

- *Authority Identification and Purpose Specification:* When collecting personal information from individuals, public bodies must inform them of the authority for collecting their information and the purpose for collecting it, as well as identify an officer or employee who can answer questions about the collection.
- *Openness and Accountability:* Public bodies should be prepared to inform individuals about what personal information is in their custody and how they manage it. They should also be prepared to demonstrate that their record-keeping practices comply with the Act, other legislation and records management policy, and answer questions or address concerns that individuals might have.
- *Informed Consent for Disclosure:* In some cases, the only way the Act will permit disclosure is with consent. In cases where the Act would permit disclosure without consent, public bodies should consider obtaining consent whenever practical, unless the public body would still need to disclose the information regardless of whether consent was granted (i.e. for the purpose of essential health care). In cases where disclosure is not essential, individuals will feel more at ease in disclosing personal information if they feel that they have a say in how it is being handled. Some program areas already operate under such a policy. Moreover, consent must be “informed” in the sense that individuals understand the reasons for any anticipated disclosure of their information.

3. Access and Correction

Individuals have a general right of access to their own personal information and to request correction of it. In order to ensure that public bodies have complied with the Act in the collection, use, and disclosure of personal information, individuals must be able to find out what information about them has been collected. Granting access to individuals also helps to enhance the accuracy of the information held and thus reduce the probability of any decisions being based on erroneous information.

Although individuals are provided the opportunity to verify the accuracy of their own information, and request correction of it, public bodies must attempt to determine whether the request for correction is warranted.

Moreover, only factual information may be corrected (e.g. date of birth, whether the individual is taking a particular medication, etc.). Opinions, including evaluations about the individual, cannot be “corrected”, even if the individual disagrees with them.

In cases where the public body determines that the applicant’s requested correction is not warranted, the Act requires that an annotation of the requested correction be placed in the record. This should be done in a way that would indicate to users of the record necessary information about the request for correction. It would be useful to include in the file a copy of the written request.

4. Limitations on the Use of Personal Information

Use of a record refers to access being made by employees in the program area of the public body that holds the information. *Section 32 of the Act restricts the use of personal information to the purpose for which it was collected; a consistent purpose; purposes to which the individual consents; and other limited circumstances.*

If you contemplate using the information for purposes other than that for which it was collected, contact your DMIP or FOI Coordinator to ensure that it complies with the Act.

Personal information should be shared within public bodies only on a “need to know” basis. This requires drawing a distinction between what employees really need to know and what they merely would like to know. Access to personal information should be made only by those employees who require this information to perform their duties. In cases of sensitive information like psychiatric records, documenting employee access in a log might assist the public body in controlling access to the record. In designing or purchasing automated systems, public bodies should consider adopting one that includes the capability of providing an audit trail of access to individual files. These measures would promote accountability for the use of such records.

5. Limitations on the Disclosure of Personal Information

Disclosure of information means the release of information in a record to other than employees in the program area of the public body that holds the record. *Section 33 of the Act permits the disclosure of personal information only under certain stipulated conditions.* This does not mean, however, that public bodies *must* disclose (or even that they *should* disclose), if these conditions are met. Public bodies should make an informed decision considering all of the relevant circumstances before disclosing the personal information. These considerations should include whether disclosure is in the interest of the individual or the public generally, and whether the disclosure is absolutely necessary for program delivery. It is important to realize that some disclosures of personal information, even in accordance with the Act, may have detrimental consequences for the individual concerned. The potential harm of disclosure must be weighed against the expected benefit of disclosure. If decision-makers do not have sufficient knowledge or experience to make these determinations, they should obtain advice from their DMIP or FOI Coordinator.

When public bodies receive requests for personal information from other public bodies or private agencies, they should verify the authority for the disclosure. For example, if the authority is an enactment, the public body should require the requester to identify that authority by direct reference to the enactment. *It is important to remember that the onus is on the public body disclosing the information to ensure that the disclosure complies with the Act.*

6. Limitations on the Retention of Personal Information

Public bodies should retain records containing personal information only for the period authorized by existing legislation or policy and then destroy them. This is important because individuals essentially have traded away their privacy in providing public bodies with personal information in order to obtain the services offered by the public body. Once these services have terminated and the legal retention period has passed, individuals have a “right to be forgotten” in that they have a right to have their privacy restored. Public bodies should be knowledgeable about records retention requirements. Retaining records beyond operational requirements can have serious consequences: once the records have ceased to be of use to the public body, they become merely a security liability, in that they continue to pose a risk of unauthorized access or disclosure that could be harmful to the individual. Moreover, records retained beyond the required retention period remain subject to a request under the Act.

7. Security

Public bodies must provide adequate security to prevent unauthorized access, collection, use, disclosure or disposal of personal information. The level of security measures should be consistent with the level of the sensitivity of the information. There are a number of reasonable security measures that public bodies should consider adopting:

Guide To Good Privacy Practices

- Employees should not leave files open on desks or in places where other employees or members of the public may see them. Files should be stored in a secure location with restricted access, such as a locked room or a locked filing cabinet. Care should also be taken in moving files to off-site storage or destruction facilities to ensure that all files reach their intended destination intact and without unauthorized access or disclosure.
- Security measures should also be employed for electronic information systems. E-mail systems should be protected by user IDs and passwords, and it is useful to have password protected screen savers on terminals. Voice mail and telephone answering machines create records. In cases where these systems are shared by employees, public bodies should limit who may have access to recorded messages left for individual employees because there are privacy considerations. It is also useful to adopt a policy of clearing messages off the system when they are no longer required to be retained.
- Personal information should not be sent by fax, unless it is absolutely necessary to transmit information quickly. In addition, sufficient precautions should be taken to ensure that it is received only by its intended recipient. These precautions include: using a secure, encrypted fax machine where available; making direct phone contact with the recipient prior to transmission to ensure that the recipient will be present at the machine when the transmission is received; confirming receipt by telephone; using an identification code control feature; taking out the paper tray at the end of the day to prevent messages from being read by maintenance staff; and ensuring that the fax number is current. The fax transmission cover sheet should state clearly the name, position, and telephone number of both the recipient and the sender and that the material is “strictly confidential”. It should also contain a message requesting that, if the fax was received in error, the recipient notify the sender and destroy the document.

Breaches in document security can cause harm to individuals and embarrassment to the public body. The media has reported a number of cases of lapses in document security including files sent for destruction being used as props on a movie set, hospital records washing up on the seashore, and copies of unsevered records containing sensitive third party personal information being disclosed to an applicant. These examples illustrate the need to take security seriously. Once information has been disclosed, there is no way to control further dissemination.

POWERS OF THE COMMISSIONER OF INFORMATION AND PRIVACY

Public bodies should be aware that the Act grants the Commissioner a number of broad powers with respect to privacy. It is important to understand the nature of these powers and the circumstances in which they might be exercised.

1. The Commissioner has the specific power to investigate and attempt to resolve complaints that personal information has been collected, used or disclosed by a public body in contravention of Part 3 of the Act. For example, an individual might complain that their information was disclosed improperly from one public body to another. After an

Guide To Good Privacy Practices

investigation into a complaint, the Commissioner may issue an order to require a public body to stop collecting, using or disclosing personal information in contravention of the Act or to destroy personal information collected in contravention of the Act.

2. The Act also grants general powers to the Commissioner to comment on the privacy implications of proposed legislation, automated systems, and records management practices. While this does not grant the power to issue binding orders in relation to these matters, by commenting on them the Commissioner may heighten public awareness about the privacy implications of these initiatives, which could create issues for the public bodies involved.

If you have any questions about this guide or any other issues surrounding privacy, contact your public body DMIP or FOI Coordinator.