OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

FAXING AND EMAILING PERSONAL INFORMATION

Replaces: *Guidelines for the Secure Transmission of Personal Information by Fax* (1996)

February 2005

Media stories confirm that mistakes in faxing and emailing personal information occur more than they should. British Columbia law requires steps to be taken to reduce risks associated with faxing or emailing of personal information. Private sector organizations covered by the *Personal Information Protection Act* (PIPA) and public bodies covered by the *Freedom of Information and Protection of Privacy Act* (FOIPPA) are required to take reasonable measures to protect personal information from risks such as unauthorized collection, use or disclosure.

A good rule of thumb is that you should only fax or email personal information that you would feel comfortable discussing over the telephone if it were your own personal information. You should not fax or email sensitive personal information such as health information or financial information unless it is absolutely necessary to send it at once and faxing or emailing is the only timely way to do so.

Common sense measures can and should be taken to reduce the risks of unauthorized collection, use or disclosure of personal information through faxing and emailing and tips found below are intended to help reduce those risks.

The following tips apply to faxing and emailing of "personal information", which is "information about an identifiable individual". The word "organization" is used below to refer to both organizations under PIPA and public bodies under FOIPPA.

This document has benefited from publications of the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner for Alberta and the Office of the Information and Privacy Commissioner for Ontario.

Please read the important notice at the end of this document about the nature and status of this document.

TIPS FOR FAXING AND EMAILING PERSONAL INFORMATION

- You should set rules about the types of information that can be faxed or emailed by or to your organization. Check regularly to make sure your employees are obeying the rules. Document your rules and also document your regular reviews of staff compliance.

- Where feasible, make one person responsible for sending and receiving personal information, especially faxes. Train that person in proper procedures and ensure they're aware of the legal duty to protect personal information.

- Any fax machine used to send or receive personal information should be located in a place that prevents unauthorized persons from seeing faxed personal information. Access to the machine should be controlled.

- Always use a fax cover sheet. The cover sheet should clearly identify the sender (with call-back particulars for the sender) and the intended recipient. It should specify the total number of pages being sent. The cover sheet should also contain a confidentiality clause saying that the faxed material is confidential, is intended only for the stated recipient, and is not to be disclosed to or used by anyone else. The confidentiality clause should ask anyone who receives the fax in error to immediately notify the sender and then return or securely destroy the personal information, as the sender requests.

- Before you fax personal information, confirm that its recipient has taken appropriate precautions to protect the personal information upon receipt. (See below for specific tips on protecting faxed personal information upon receipt.)

- Before faxing or emailing personal information, confirm that you have the correct fax number or e-mail address for your intended recipient.

- If you use pre-programmed fax numbers, regularly check to ensure that the fax numbers are accurate and up to date.

- After you have dialled a fax number, carefully check the number you dialled before sending the fax. This also applies when using pre-programmed fax numbers.

- You should check each fax confirmation report at once to be sure the fax went to the right place—check the number on the report against the recipient's number. Also check the number of pages actually transmitted and received.

- If you've designated one person to send and receive faxes, have that person check each day's fax history report for errors or unauthorized faxing. Keep fax confirmation sheets and fax history reports long enough to do this.

- Retrieve material you are sending by fax from the fax machine as soon as it has been processed for sending. Don't leave it sitting on or near the fax machine. When you're faxing sensitive personal information, stay by the machine at all times during faxing.

- If you must fax or email sensitive personal information such as health information or financial information, consider phoning first to confirm that the intended recipient is actually the right person to receive the fax to confirm, that the recipient will be there to receive the fax, and to confirm the recipient's fax number. Ask the intended recipient to call to confirm receipt of the fax.

- When faxing or emailing sensitive personal information, consider the use of unique identifiers or codes to protect the identity of the individuals involved.

- If you receive a fax in error, promptly notify the sender and return or destroy the information, as requested by the sender.

- When receiving a fax, check the number of pages you've actually received against the number of pages noted on the fax cover sheet. Check to ensure you haven't received any material you shouldn't be getting. If you do receive material you shouldn't be getting, promptly notify the sender and return or destroy the information, as requested by the sender.

- If your fax machine has a feature that requires the recipient to enter a password before the recipient's machine will print the fax, use that feature for sensitive personal information at least. Similarly, the recipient could arrange for the sender to make sure the recipient must supply a password to retrieve faxes of personal information.

- If you fax sensitive personal information, consider using secure fax machines that employ encryption or other security measures.

- If you use computers for sending, receiving or storing faxes, create appropriate computer directories and passwords so that faxes can only be sent, received and accessed by designated users, using secret passwords. Before faxing personal information by computer modem, check that the recipient's computer is protected in the same way.

- Do not make or keep more copies of faxed or emailed material than you truly need. Securely destroy extra copies.

- If someone asks you to fax or email their personal information to them, first explain to them how faxing or emailing risks their personal information being accidentally disclosed or deliberately intercepted by other people and get their consent before you fax or email their personal information.

- If personal information is mistakenly faxed or emailed to the wrong person, or is otherwise compromised through faxing or emailing, and you can't get the information back, notify your supervisor and the person responsible for privacy compliance in your organization and notify the OIPC of the incident. Your organization or public body should promptly notify the individual(s) whose personal information has been compromised, telling them the kind of information that has been compromised and steps that are being taken.

- Never use email distribution lists to email personal information.

- Remember, email is like sending a postcard. The content of an email can be read during its transmission. When emailing personal information—especially sensitive information such as health information—you should encrypt it so only the intended recipient can read it. Free or low-cost encryption software is readily available on the Internet or through retailers.

- Each email mailbox used to send or receive personal information should have a secure password known only by the employee authorized to access that mailbox. In case of a common mailbox, only employees authorized to access it should know the password.

- Consider deleting emails from your computer a reasonable time after successful sending and retain only paper copies.

OTHER RESOURCES

Other resources are available to help you meet your obligations regarding faxing or emailing of personal information, including the following:

- Office of the Information and Privacy Commissioner for Alberta, *Guidelines on Facsimile Transmission*: www.oipc.ab.ca/ims/client/upload/Guidelines_on_Facsimile_Transmission.pdf

- Office of the Information and Privacy Commissioner/Ontario, *Guidelines on Facsimile Transmission Security*: www.ipc.on.ca/docs/fax-gd-e.pdf

- Office of the Privacy Commissioner of Canada, *Faxing Personal Information*: http://www.privcom.gc.ca/fs-fi/02_05_d_04_e.asp.

- Commission d'accès à l'information du Québec: http://www.cai.gouv.qc.ca/06_documentation/01_pdf/mail.pdf