



Use of Fax by Physicians

This section will:

- Summarize the benefits and risks associated with using a fax in the clinical context.
- Identify key considerations when using faxes to transmit personal information.

In today's clinical setting, faxes are commonly used to transmit health information. For example, a laboratory may fax a patient's medical test result to a physician, or a physician may fax a copy of the patient's medical record to a specialist who intends to treat the patient.

Under the BC Personal Information Protection Act (PIPA) steps must be taken to reduce the risks associated with faxing personal information and reasonable safeguards must be in place to protect personal information from unauthorized collection, use, and disclosure.

What Are the Risks?

Faxing increases the risk that sensitive personal information could be read by individuals other than those for whom they were intended. This might occur when, for example, personal health information such as a medical diagnosis, is sent to an incorrect fax number (caused by misdialing or by pressing the wrong speed-dial key), or when information is exposed to unauthorized individuals simply because the fax machine is located in an open, unsecured location. Fax transmissions can also be tapped into and monitored similar to a telephone call.

How to Reduce the Risks

A fax sent to another physician or hospital about urgent or significant patient issues should not be considered a substitute for effective and efficient communication. Faxes can be missed, may not reach their designation, or may remain in receiving trays if the recipient is unavailable. Here are some steps to reduce the risks:

1. Establish an office policy on faxing and ensure that staff are trained on the appropriate use of the fax machine and faxed documents.



2. Fax personal health information only when it is absolutely necessary and when the information must be transmitted immediately, and only if the information is something that could be comfortably discussed over the telephone with a patient.
3. Ensure that any fax machine used to send or receive personal information is “dedicated” and located in a secure area to prevent unauthorized persons from viewing or receiving the documents. Sharing fax machines, particularly where personal information is frequently sent and received, is discouraged.
4. If sending personal information by fax modem (a fax device contained in a computer), confirm that the other users of the computer cannot access the fax program without a password. Consider using encryption.
5. Always use a fax cover sheet that identifies both the sender and recipient with contact information and states the total number of pages being sent.
6. Include a disclaimer stating that the faxed material is confidential and only intended for the stated recipient. This disclaimer should also state that anyone receiving the fax in error must immediately notify the sender and return or destroy the fax, as per the request of the sender.
7. Before faxing the information, confirm the recipient’s fax number and ensure that the recipient has taken appropriate precautions to protect the personal information upon receiving it.
8. If using pre-programmed fax numbers, regularly verify these numbers to ensure they are accurate and up-to-date.
9. After dialling a fax number, including a pre-programmed number, confirm the number before sending the fax.
10. Remove documents sent by fax as soon as they have been processed. Do not leave the material sitting on or near the fax machine.
11. Check the fax confirmation report as soon as the fax has been sent to confirm that the fax went to the correct place and that all pages were transmitted and received.
12. If a fax is received in error, promptly notify the sender and return or destroy the information as requested by the sender.

If a fax containing personal information is sent to the wrong number or person, follow these steps:

1. If the information cannot be retrieved or destroyed, notify the person responsible for privacy compliance in the office.
2. Follow procedures for managing privacy breaches. (See the section [Responding to a Privacy Breach—Key Steps for Physicians](#)).



If someone asks the physician's office to fax his or her personal information, be sure to follow these steps:

1. Identify the person making the request with certainty and advise him or her of the preference to provide the data in a more secure fashion (e.g., photocopies sent by mail or courier).
2. Explain how faxing personal information can result in accidental disclosure or interception by other people not intended to receive it.
3. Explain the precautions that have been taken to reduce the risks and ensure the person consents before the personal information is faxed.

Maintenance of Faxed Documents

When planning a document maintenance policy, consider the following:

1. Do not make or keep more copies of faxed material than needed.
2. Securely destroy extra copies that are no longer needed.
3. Ensure that personal health information that has been faxed becomes part of the patient's medical record and follow appropriate retention guidelines.

As well, consider these additional factors:

1. Where possible, use alternative and secure methods of delivering personal information, particularly if it is sensitive.
2. If faxing sensitive personal information on a frequent basis, use a secure fax machine that has encryption and other security measures.
3. Use the feature that requires the receiver to enter a password before the machine will print the fax to ensure that only the intended receiver can retrieve the document.
4. Appoint one individual in the office to be responsible for sending and receiving faxes. This individual can check each day's fax history report for errors or unauthorized faxing.
5. Arrange a time to receive faxes so that someone can be at the fax machine when they arrive.
6. Phone the recipient to confirm that he or she is the right person to receive the fax, that he or she will be there to receive the fax, and to confirm the fax number. Have the recipient call back to confirm receipt.
7. Use unique identifiers or codes to protect the identity of the individual whose personal information is being sent by fax.