Guide to Faxing

Preventing Breaches with Safeguards and Responding to a Privacy Breach

Guidance on what safeguards public bodies and trustees need to have in place when faxing personal information and personal health information and what to do when efforts fall short and faxes go astray resulting in a privacy breach.

DISCLAIMER This document is not intended to provide legal advice and is provided for informational use only

January 2026

Office of the
Saskatchewan Information
and Privacy Commissioner

In Saskatchewan, government institutions, local authorities (public bodies) and trustees have a legislated duty to protect personal information (PI) and personal health information (PHI) through *The Freedom of Information and Protection of Privacy Act* (*FOIP*), *The Local Authority Freedom of Information and Protection of Privacy Act* (*LA FOIP*) and *The Health Information Protection Act* (*HIPA*).

This guide offers a list of necessary safeguards to have in place when faxing PI/PHI, what to do when a misdirected fax is sent or received, and what to expect in an investigation by the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).

Privacy breaches by fax occur for a variety of reasons, including user error or failure to update systems. Privacy breaches of this nature, however, are preventable. As such, steps should be taken to prevent a privacy breach from occurring in the first place, including providing ongoing education to staff, and exploring alternative methods of transmitting PI/PHI such as using encrypted file sharing or other secure, electronic methods.[1]

This guide also offers a checklist for public bodies and trustees to refer to when a misdirected fax is received or sent.

What is a Misdirected Fax?

A misdirected fax is a fax containing PI/PHI that is received by an unintended recipient without the requisite need-to-know. A misdirected fax results in a privacy breach.

Misdirected faxes often occur for the following reasons:[2]

- **Human error** – Entering fax numbers incorrectly, relying on auto-suggest functions that bring up the wrong number or searching for the number on the Internet without verifying if the site and number chosen are correct. This can result in sending PI/PHI to the wrong number and being received by an unintended recipient.
- **Lack of control over who is at the receiving end** - Even if sending a fax to the correct number, if the receiving end does not have proper safeguards, PI/PHI can be viewed by an unintended recipient. For example, the faxed information may be left unattended, or the fax machine may be in a location where multiple people have access to it, someone without the need-to-know could access.

[1] Northwest Territories Information and Privacy Commissioner Review Recommendation 10-091 at paragraph at page 3.

[2] OIPC Investigation Report 032-2022 at paragraphs [36] to [39] discussed several ways or reasons that misdirected faxes occurred that came to the attention of OPIC.

- **Out-of-date contact information** - Public bodies or trustees may rely on pre-programed fax numbers from directories or electronic health records that are not kept updated. By not keeping these current, a fax can be directed to an incorrect location.

Note for trustees: even if a misdirected fax is received by another trustee (e.g., a physician) who is not the intended recipient or who does not have a need-to-know, it still qualifies as a privacy breach.

What is Personal Information and Personal Health Information?

Personal information is defined at section 23(1) of *LA FOIP* and at section 24(1) of *FOIP*, though the lists provided are not exhaustive. Personal information is information that is:

- About an identifiable individual, meaning the individual is capable of being identified from the information (e.g., direct identifiers such as their name or address are given).
- Personal in nature.

Information can be personal information even if, in the absence of a name or other direct identifier, a person can reasonably be identified by the data elements.

Personal health information is defined at section 2(1)(m) of *HIPA*, and includes:

- Information with respect to the physical or mental health of an individual.
- Information with respect to any health service provided to an individual.
- Information regarding the donation by an individual of any bodily part or bodily substance or information derived from the testing or examination of a bodily part or substance (e.g., x-ray, lab-test results).
- Information that is collected in the course of providing health services to an individual, or incidentally to the provision of health services to the individual.
- Registration information.[3]

[3] "Registration information" in *HIPA* means information collected about an individual that is collected for the purpose of registering the individual for a health service and includes their health services number (HSN) and any other number assigned to the individual aspart of a system or unique identifying numbers prescribed in *HIPA Regulations*. It can include tombstone information that is collected when registering an individual for a health service, such as your address and phone number.

The Health Information Protection Regulations, 2023 (*HIPA Regulations*) also define PHI to include genetic testing information, including that of the subject individual or of their family members. It also includes an individual's family medical history.

The Importance of Safeguards for Faxing

Public bodies and trustees often use fax machines to transmit client or patient information because of the speed and convenience.

Faxing documents that contain highly sensitive PI/PHI such as Social Insurance Numbers, HSN, banking information, lab results or other medical information, etc., to an unintended recipient can have significant consequences for the subject individual. Consequences can range from identity theft to the disruption of the individual's continuity of care. This is why misdirected faxes need to be taken seriously, and reasonable safeguards put in place to prevent. These are also required by law as follows:

- Sections 24.1 of *FOIP*/23.1 *LA FOIP* state that public bodies have a duty to protect PI that is in their possession or under their control.[4] They must establish policies and procedures to maintain administrative, technical and physical safeguards. Safeguards are intended to protect against threats or hazards to, loss of, unauthorized access to or use of, disclosure or modification of PI.

- Section 16 of *HIPA* requires trustees to have reasonable safeguards in place to protect PHI in their custody or control. Trustees must establish policies and procedures to maintain administrative, technical and physical safeguards. Safeguards are intended to protect against threats or hazards to, loss of, unauthorized access to or use of, disclosure or modification of PHI.

Safeguards include:

- **Administrative safeguards** are controls that focus on internal organization, policies, procedures, work standards and maintenance of security measures that protect PI/PHI. Administrative safeguards include written policies and procedures, annual training for employees, confidentiality agreements, agreements with IMSPs, auditing programs, records retention and destruction schedules and access restrictions.

- **Technical safeguards** are the technologies that protect personal health information and control access to it. Examples include user identifications, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital information systems.

[4] "Possession" means the physical possession of a record plus a measure of control. "Control" connotes authority, or the authority to manage a record including restricting, regulating and administering its use, disclosure or disposition. Possession and custody are interchangeable terms.

- **Physical safeguards** are physical measures including locked filing cabinets, offices and storage rooms, alarm systems and clean desk approaches.

Implementing Appropriate Safeguards for Faxing

Public bodies and trustees need safeguards for faxing as faxing increases the risk of a privacy breach. The following safeguards can help lower the risk:

1. Adopt Written Policies, Procedures and/or work standards on Faxing (Administrative Safeguards)

- Include references to applicable privacy legislation in your organization's policies and procedures.
- Include the types of PI/PHI that can be faxed by your organization, or that your organization can receive.
- Ensure that employees, including all new employees, are trained on the policy /practices and are regularly reminded of it.
- Post reminders about key policies and procedures near fax machines.
- If possible, designate one employee to be responsible for sending and receiving PI/PHI by fax. Train that employee in proper procedures to ensure they are aware of the legal duty to protect the information.

2. Take Steps to Fax Safely (Administrative Safeguards)

- Determine if you need to fax, such as because of a time requirement, or if you can forward the information in another way that is also quick but more secure.
- If someone requests that their PI/PHI be faxed, explain to them the risk that their information may be deliberately intercepted by people other than the intended recipient. Seek their consent before faxing.
- If possible, remove all personal identifiers and confidential information before faxing the information.
- Confirm that you have the recipient's correct fax number. Confirm the number with the intended recipient prior to faxing. Also confirm that the recipient has taken appropriate precautions on their end to prevent those without a need-to-know from viewing the faxed document.
- Always use a fax cover sheet that clearly identifies or includes:
    - The name of sender.
    - The contact information for the sender.

    - The name of the intended recipient
    - The recipient's fax number.
    - The total number of pages being sent.
    - A confidentiality clause that specifies that the faxed material is confidential, intended only for the stated recipient, and not to be used or disclosed by any other individual. The clause should state that if a fax is received in error, the recipient should immediately notify the sender and then return or securely destroy the fax.
- After entering the fax number, doublecheck the number before hitting "send".
- Check the fax confirmation report to be certain that the fax went to the right place – check the number on the report against the confirmed recipient's number. Also check the number of pages transmitted and received. If you have designated one employee for faxing, that individual should check each day's fax history reports for errors or unauthorized faxes.
- If the fax contains highly sensitive information follow-up with a call after the fax is sent to ensure it was received.
- When faxing PI/PHI, stay by the machine to ensure that all materials were transmitted correctly and that fax isn't left where others without a need-to-know are able to view its contents.

3. How to Treat Faxes you Receive (Administrative Safeguards)

- Retrieve faxes immediately but only if clear from the cover page that you are not the intended recipient and deliver to the intended recipient or individual with a need-to-know. Do not review any content.
- Never leave faxes sitting on or near the fax machine.
- Take security precautions for faxes received after normal business hours. Ensure those without a need-to-know do not have access to the fax machine when it is unattended (e.g., cleaning staff).

4. Setting Up and Maintaining your Fax Machine (Technical and Physical Safeguards)

- Ensure your fax machine prints a header at the top of each page that includes the fax number and date and time. Update the header when your fax number or office information changes.
- Use a fax machine that has enhanced security features such as encryption or other heightened security measures.

- Place your fax machine in an area of the office that prevents unauthorized individuals from viewing/retrieving faxes. Control who has access to the machine.
- If you give up a fax number, it can eventually be reassigned to another individual or company. If you do not want the number to be used while you advise clients that the organization is moving or closing, check with your telephone provider about renting the number for an interim period. This will allow time to contact all clients and to update them.
- Fax machines (including multi-function devices) have hard drives and/or memory that store and retain data. When disposing of, returning at the end of a lease or selling a fax machine, properly scrub the hard drive to remove all stored information or securely destroy as appropriate depending on sensitivity of information.[5]
- Pre-program only fax numbers that are commonly used and be sure to check those numbers regularly to ensure they are accurate and current.
- If you move or if your fax number is changed, immediately provide your contacts with your updated fax number, and update all directories and websites that include the previous number. Destroy pre-printed forms, fax cover sheets, and correspondence that refer to your previous number, including letterhead, business cards, prescription forms, etc.

When OIPC Will Investigate a Privacy Breach

OIPC has a legislated mandate to investigate privacy breaches and ensure they are properly managed. OIPC can learn of a privacy breach and begin an investigation in several ways, including:

- From a citizen whose information has been breached by a public body or trustee.
- By a third party who receives a misdirected fax.
- From media alerts or announcements.
- From the public body or trustee (proactively reported).

If You are an Unintended Recipient

At times, an individual or organization may receive a fax that is not intended for them.

[5] See resources: *Sanitization and Disposal of Electronic Devices*; *How to Prepare your Device - Recycle My Electronics Saskatchewan*, *Disposing of Your Electronic Media* | Information and Privacy Commissioner of Ontario

While it may be a one-off occurrence because of sender error, there are times when the same public body or trustee may continually send faxes to the same unintended recipient – this may speak to a larger systematic issue that the public body or trustee is either not aware of or has not taken steps to address.[6]

If you receive a misdirected fax, the first thing you should do is review the fax cover page or header information for contact information. Contact the public body or trustee to determine who their privacy officer is. Let the privacy officer know details about what you received and ask how they will manage the breach. Options include: the public body or trustee can send someone to pick up the misdirected fax, or they may ask you to securely destroy it. If you are asked to securely destroy the information, you should confirm with the public body or trustee that you have done so and how. If you are able, you could also hand deliver the fax to ensure it ends up in the right hands. As an unintended recipient if you do not assist in containment, you may be exacerbating the breach. If the public body or trustee does not take steps to contain the breach, at that point, you may contact the OIPC for guidance.

If You are a Public Body or Trustee

A public body or trustee should consider proactively reporting a privacy breach by misdirected fax to OIPC that it was responsible for a variety reasons. It may reduce the chance that OIPC will issue a public investigation report on the matter as provides OIPC with an opportunity to provide support and guidance to the public body or trustee at early stages. Doing so also allows the public body or trustee to assure affected individuals or media that OIPC is engaged.

When OIPC investigates a privacy breach that is proactively reported where a breach is confirmed, there are three possible outcomes:

- If OIPC is satisfied with how the public body or trustee managed the breach, then the file may be closed informally, and no public investigation report is issued.
- If OIPC is not satisfied with how the public body or trustee managed the breach, if the breach is egregious, if there are systematic issues, if there is a significant number of affected individuals, or if there is educational value in doing so, OIPC will issue a public investigation report.
- If there are affected individuals who make a formal complaint, OIPC will advise the public body or trustee that a public investigation report will be issued. If a complainant comes forward, OIPC will typically open a file and advise the public body or trustee accordingly.

[6] OIPC Investigation Report 032-2022 at paragraphs [37] and [38].

To proactively report a privacy breach, public bodies and trustees can use the following form – *Proactively Reported Breach of Privacy Reporting Form for Public Bodies.*

For more information, see OIPC's resource, *Privacy Breach Guidelines*.

What to Expect in an Investigation by OIPC

If an affected individual or third party (witness) makes OIPC aware of a privacy breach involving misdirected faxes that warrants further investigation, OIPC will open a file and inform the responsible public body or trustee, in writing, of a formal investigation after early resolution efforts are attempted.

In the notice of investigation, OIPC will ask the public body and trustees to complete and return OIPC's *Privacy Breach Investigation Questionnaire* (Questionnaire) and provide other relevant material within 30 days (e.g., relevant policies, procedures, work standards).The Questionnaire walks public bodies and trustees through the four best practice steps for responding to a breach (containment, notification, investigation, and prevention). If further information is required at any point in the investigation, OIPC will advise.

After concluding the investigation, a public investigation report may be issued.

Other helpful resources include OIPC's:

- *Privacy Breach Guidelines for Government Institutions and Local Authorities*.
- *Privacy Breach Guidelines for Trustees*

Attached to this guide are also checklists for recipients of a misdirected fax and public bodies/trustees who send one to use in managing a breach caused by misdirected fax.

Checklist

If you receive a misdirected fax[7]

☐	Is your organization/are you the intended recipient, or do you have a need-to-know? If yes, no need to go any further. If no, move to the next step in this Checklist.
☐	Have you notified your organization's privacy officer of a possible privacy breach?
☐	Have you determined who the sender is from the fax cover sheet or header information?
☐	Have you contacted the sender to advise them of the breach, so they are aware of it?
☐	If possible, have you spoken to the sending organization's privacy officer so they can log and investigate the incident, and implement safeguards to prevent similar breaches?
☐	Have you advised the sender on how to contain the breach and what to do with the misdirected fax? For example, ask if they would like it returned to them by mail, securely destroyed by you, or if someone will retrieve it.
☐	Have you confirmed with the sender that you will not keep a copy/securely dispose of the misdirected fax once the sender is clear on what was sent in error?
☐	If the sender asks, have you confirmed with them that you will not forward the misdirected fax to the intended recipient on their behalf? Doing so may compound the problem, so it is better that the sender re-sends the fax themselves.
☐	If dissatisfied with interactions with the sender, have you considered if you will notify OIPC?

[7] Only individuals in an organization tasked with responsibility for managing or addressing a privacy breach should take certain actions.

If you send a misdirected fax

☐	Have you contacted your organization's privacy officer for guidance and support? For guidance, you may also consult OIPC's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Health Trustees*.
☐	Have you taken steps to contain the breach? This includes: • Immediately contacting the organization where you sent the misdirected fax and confirming that they received it. • Explaining that the fax was sent in error and contains PI/PHI. • If you have the original document, asking the recipient if they can securely destroy the misdirected fax (e.g., by using a cross-cut shredder), and ask them to confirm destruction. • If they can't destroy it, asking them to return it by mail or bring to you, or letting them know you will physically retrieve it (e.g., send a courier or a staff member). • Asking the recipient not to keep copies of the misdirected fax and confirming that they haven't. • Informing the recipient of OIPC's role and mandate if they have questions or concerns. • Documenting the conversation.
☐	If you re-send the fax, have you ensured you are sending it to the correct recipient's fax number?
☐	Have you notified the affected individuals as soon as possible about the breach? Notification is mandatory (*FOIP* and *LA FOIP*) if the incident creates a real risk of significant harm to the individual, such as if there is a possibility for identity theft.[8] Contact OIPC if you are unsure about this step.
☐	Have you investigated why the breach occurred, or determined the root cause? What actions led to the breach occurring? • Did you review policies and procedures to ensure best practices were followed? Are policies and procedures adequate? • Have you determined if employees involved in the breach are aware of the policies and procedures, and properly trained? • Have you analyzed the breach and determined what the associated risks are for the affected individual and the organization? • Have you completed an investigation report that includes ways to make sure the same type of breach doesn't happen again?

[8] See section 28.1 of *LA FOIP* or section 29.1 of *FOIP*; *HIPA* does not have a comparable provision.

Acknowledgments

- *Guidelines on Facsimile Transmission*, Office of the Alberta Information and Privacy Commissioner (www.oipc.ab.ca).

- *Faxing and Emailing Personal Information*, Office of the British Columbia Information and Privacy Commissioner (www.oipc.bc.ca).

- *Manitoba Ombudsman Practice Note: Privacy Considerations for Faxing Personal Information and Personal Health Information*.

- *Fact Sheet: Faxing Personal Information*, Office of the Privacy Commissioner of Canada (www.priv.gc.ca).

Contact Information

If you have any questions or concerns, please contact the OIPC at:

306-787-8350 | toll free 1-877-748-2298
503 – 1801 Hamilton Street | Regina SK S4P 4B4

intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC