FAXING PI AND PHI

Safeguards and responding to a breach

This guide assists public bodies and health trustees to ensure the necessary safeguards are in place when choosing to send personal information (pi) and personal health information (phi) by fax. It also provides a checklist of things to do when a misdirected fax is sent or received.

Office of the
Saskatchewan Information
and Privacy Commissioner

SEPTEMBER 2020

In Saskatchewan, government institutions, local authorities and health trustees have a duty to protect personal information and personal health information 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). The following guide provides a list of appropriate safeguards when using fax to transmit personal information and personal health information, what to do when a misdirected fax is sent or received and what to expect in an investigation by the Information and Privacy Commissioner (IPC).

WHY ARE SAFEGUARDS FOR FAXING NECESSARY?

Faxing personal information or personal health information increases the risk of an unauthorized collection, use or disclosure of this information. Some reasons for these risks include:

- **Human error:** we can easily make an error when entering a 10 digit fax number into the fax machine, or using auto-suggest functions, sending personal information/personal health information to the wrong number resulting in it being received by an unintended recipient without a legitimate need to know.
- **Lack of control**: even when a fax is sent to the correct number, without proper safeguards on the receiving end, personal information/personal health information could be viewed by an unintended recipient (ex. the faxed information is left unattended or the fax machine is located in an area where multiple people have access to it).
- **Out-of-date contact information:** many public bodies rely on pre-programed fax machines or fax numbers from electronic health records or directories that may be out of date causing a fax to be directed to someone without a need to know.

WHAT IS A MISDIRECTED FAX?

A "misdirected fax" is a fax containing personal information or personal health information that is received by an individual without a need-to-know. This would result in an unauthorized disclosure of personal information or personal health information.

TRUSTEES NOTE: Even if a misdirected fax is received by another trustee, without a need-to-know, it qualifies as a privacy breach.

SAFEGUARDS FOR FAXING PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

The following are suggestions for safeguards that public bodies incorporate into their written policies and procedures.

Policies and Procedures

- Adopt a written policy on faxing personal information and personal health information and ensure that employees, including all new employees, are trained and regularly reminded of the policy.
- Policies and procedures should include specific references to applicable privacy legislation and the types of information that can be faxed by or to your organization.
- Post reminders about key points near fax machines.
- If possible, designate one employee to be responsible for sending and receiving personal information and personal health information by fax. Train that employee in proper procedures and ensure they are aware of the legal duty to protect the information.

Sending Faxes

- Determine if there is an immediate time requirement that necessitates faxing the personal information or personal health information. Is there a quick and more secure way to forward the information to the recipient?
- If the subject individual requests that their personal information or personal health information be faxed, first explain the risk of accidental disclosure or the possibility that the information may be deliberately intercepted by people other than the intended recipient and seek their consent before faxing.
- Remove all personal identifiers and confidential information before faxing the information, wherever possible.
- Before faxing personal information or personal health information, confirm that you have the correct fax number for the intended recipient and confirm with the recipient (or another employee in the office) the right number before sending.

- When faxing personal information and personal health information, confirm that the recipient has taken appropriate precautions to prevent those without the requisite need to know from viewing the faxed document.
- Always use a fax cover sheet clearly identifying the sender, the contact information for the sender, the intended recipient, the recipient's fax number and the total number of pages sent. Include a confidentiality clause that specifies that the faxed material is confidential, is intended only for the stated recipient, and is not to be used or disclosed by any other individual. The confidentiality clause should ask the individual in receipt of a fax received in error to immediately notify the sender and then return or securely destroy the personal information or personal health information (as requested by the sender).
- After the fax number has been entered carefully check 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 actually 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.
- When faxing personal information or personal health information, stay by the machine to ensure that all materials were transmitted correctly.

Receiving Faxes

- Retrieve all materials that have been faxed from the fax machine immediately and deliver to the individual with a 'need-to-know'. Do not leave faxes sitting on or near the fax machine.
- Security precautions should be taken for faxes received after normal business hours such as ensuring that no one without a need to know will have access to the fax machine if it is unattended.

Fax Equipment

- Ensure that your fax machine prints a fax header at the top of the page which includes the fax number and date and time.

- If you have a need to continually fax personal information or personal health information, look into acquiring a fax machine that has enhanced security features such as encryption or other heightened security measures.
- Fax machines should be physically located in an area of the office that prevents unauthorized individuals from viewing/retrieving faxed personal information and personal health information. Make sure to control access to the machine.
- Be aware that your fax number likely will be reassigned to another individual or company once you have given up the number. If you require the number not to be used while you advise clients that the organization is moving or closing, check with your telephone service provider about options to rent the number for a period of time to ensure all clients have been contacted and have had the opportunity to update their contact information.
- Be aware that fax machines now have hard drive and/or memories that store and retain information. When disposing of or selling a fax machine, ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory. Alternatively, ensure the machine is destroyed properly so no personal information or personal health information can be retrieved from it.
- Only pre-program commonly used fax numbers and be sure to check those numbers regularly to ensure accuracy.
- If you have pre-programmed a fax header into your fax machine that automatically prints the fax number on the recipient copy, update that information if your fax number or office contact information changes.
- Safeguarding faxes not only applies to fax equipment. If you re-locate or if your contact information is changed, ensure that you update your fax number with all of your contacts and directories that included the previous number. Don't forget to destroy pre-printed forms, fax cover sheets, and correspondence that refer to your previous number. This would include such items as letterhead, business cards, prescription forms, etc – all of which need to be replaced with updated information.

CHECKLISTS: WHAT TO DO WHEN YOU'VE SENT OR RECEIVED A MISDIRECTED FAX

Note: Tailored checklists for trustees are available in the resource *Checklists for Trustees: Misdirected Faxes* available at www.oipc.sk.ca.

What to do if you receive a misdirected fax

- ✓ Recognize that this is a significant matter with the need for some urgency to address both privacy implications and possibly continuity of care for the subject individual.
- ✓ Determine if you have a need-to-know.
- ✓ Notify your privacy officer.
- ✓ Use the fax cover sheet or fax header to determine who the sender is.
- ✓ Contact the sender to advise of the breach so they become aware of the breach.
- ✓ When possible, speak to the organization's privacy officer so that the incident can be logged and investigated and safeguards implemented if necessary to prevent similar occurrences.
- ✓ Discuss with the sender how to contain the breach and what to do with the misdirected fax (ex. return by mail, secure destruction, etc.). When possible, give the sender confirmation once the agreed upon action has been performed.
    - o Do not keep a copy of the misdirected fax.
    - o Do not attempt to forward the misdirected fax to the intended recipient as this could compound the breach. Leave that to the sender.
- ✓ Consider proactively reporting the breach by notifying the IPC who has a legislated mandate to investigate privacy breaches and ensure they are properly managed. The IPC has a reporting form for public bodies to proactively report a privacy breach to the IPC – *Proactively Reported Breach of Privacy Reporting Form for Public Bodies*.
- ✓ Factors to consider include:
    - o Is the sender identifiable?
    - o Is the personal information or personal health information particularly sensitive?
    - o Are there multiple faxes with apparent multiple senders?

- Is the problem recurring after proper steps have been taken to contain past occurrences?

✓ The IPC will ask if you have first made attempts to contact the sender and then ask that you mail in the misdirected fax with any relevant details to our office.

✓ Once the IPC opens a file, if not already provided, will also request that public body complete the IPC's *Privacy Breach Investigation Questionnaire* (*Questionnaire*).

What to do if you have sent a misdirected fax

✓ Contact your organization's privacy officer for guidance and support. Also consult the OIPC resource *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Health Trustees*.

✓ Contain the breach: immediately contact the organization(s) to which the misdirected fax(es) has been sent.

- Confirm that the fax has been received.
- Explain that the fax contains personal information or personal health information and has been sent in error.
- If you have the original fax, ask the recipient if they have the capability to destroy the personal information or personal health information securely (ex. capability to shred in a cross-cut shredder). Ask for confirmation that destruction has occurred.
- Otherwise, ask that the recipient return the personal information or personal health information by mail or send a courier for pick up.
- Request that the recipient not keep any copies of the personal information or personal health information. Ask for confirmation.
- Inform the recipient of the mandate and role of the IPC should they have further concerns or questions.
- Document the conversation.

✓ Ensure the personal information or personal health information reaches the intended recipient.

✓ Notify the affected individual(s) as soon as possible. Notification is mandatory if the incident creates a real risk of significant harm to the individual. Contact the IPC if unsure that this step is warranted.

- ✓ Once the breach has been contained investigate.
    - o Determine root cause of the breach.
    - o Review written policies and procedures on faxing personal information or personal health information to ensure that best practices were followed.
    - o Determine if the employees involved in the breach were aware of the policies and procedures and had received training.
- ✓ Analyse the breach and consider the associated risks to both the organization and affected individuals.
- ✓ Notify the IPC as soon as possible. When privacy breaches are proactively reported to the IPC, depending on the scale and severity of the breach, it will open a file to monitor the response of the public body and ensure best practises are being followed. The file is then closed once the public body's internal investigation has satisfactorily come to a close. If the breach is covered by the media, the public body will have the benefit of assuring the public it is working with the IPC.

WHAT CAN BE EXPECTED IN AN IPC INVESTIGATION

If the IPC is made aware of a privacy breach involving misdirected faxes by an affected individual or third party, the public body will be informed of a formal investigation by a written notification letter. If the breach is proactively reported by the public body, the IPC will open a file, but is more likely to result in informal resolution if all necessary steps are taken.

The IPC will request that the public body complete and provide the IPC's *Questionnaire* and other relevant material within 30 days.

The *Questionnaire* takes public bodies through the four best practice steps of responding to a breach (containment, notification, investigate, and prevent future breaches). Through this process of answering the questions, the completed *Questionnaire* should provide the IPC with what is required to conduct our investigation. If further information is required, the IPC will advise.

See the IPC's resources *Privacy Breach Guidelines for Government Institutions and Local Authorities, Privacy Breach Guidelines for Trustees* and *Privacy Breach Investigation Questionnaire* for more information of the IPC's breach of privacy investigation process (available at www.oipc.sk.ca).

CONTACT INFORMATION

If you have any questions or concerns during any stage of the review process, please contact the IPC:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

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