Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 015-2025

Saskatchewan Workers' Compensation Board

May 30, 2025

Summary: The Complainant submitted a claim to the Saskatchewan Workers' Compensation Board (WCB) by completing a "Worker's Initial Report of Injury" form. The Complainant recorded their current mailing address on the form. The WCB, however, sent several pieces of mail to the Complainant's former mailing address, which was associated with a previous claim. The Complainant emailed the WCB to advise it had been sending mail to the incorrect mailing address and provided their current mailing address. Despite the update, the WCB continued to send mail to the Complainant's former mailing address. The Complainant informed the WCB a second time that it was sending mail to the incorrect mailing address. Eventually, the WCB updated the Complainant's mailing address. The Complainant requested an investigation into the matter by the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). The Commissioner made several findings, including that privacy breaches occurred every time the WCB sent the Complainant's personal information to the incorrect mailing address, that WCB made an unsatisfactory effort to contain the privacy breaches, and that WCB lacks adequate policies and procedures for its employees to follow on meeting the requirements of section 27 of *The Freedom of Information and Protection of Privacy Act* (FOIP) and section 19 of *The Health Information Protection Act* (HIPA). The Commissioner made four recommendations to the WCB, all to be completed within 30 days of issuance of this Investigation Report. These included contacting the recipient at the Complainant's former mailing address with a request that they return the mail that the WCB had not yet recovered, and that the WCB develop policies and procedures that guide its employees on how to meet the requirements of section 27 of FOIP and section 19 of HIPA. The Commissioner also recommended that the WCB send a written apology to the Complainant for repeatedly breaching their privacy.

I BACKGROUND

[1] To submit a claim to the Saskatchewan Workers' Compensation Board (WCB), the Complainant completed a WCB form titled, "Worker's Initial Report of Injury" and dated it September 8, 2023. On this form, the Complainant recorded their current mailing address.

[2] On January 9, 2024, WCB mailed a payment statement to the Complainant. However, the WCB sent the payment statement to the Complainant's former mailing address, which was associated with a previous claim. The WCB sent mail to the Complainant's former address again on January 10, 2024, and on January 26, 2024, and two further items were mailed to the Complainant's incorrect address on February 5, 2024. In total the WCB sent five pieces of mail to the incorrect address.

[3] On March 25, 2024, a WCB employee emailed the Complainant. Attached to the email were copies of returned mail. The WCB employee asked the Complainant to confirm their mailing address.

[4] On the same day, the Complainant responded to the WCB employee. The Complainant said:

> That is a really old mailing address which would have been attached to my previous claim.
>
> My mailing address is [Complainant's current mailing address]
>
> I have received mail from wcb with my current address, so I'm not sure what happened with this one.

[5] On the same day, the WCB employee responded, "Okay thank you."

[6] On May 3, 2024, the WCB again mailed a letter to the Complainant's former mailing address.

[7] On June 5, 2024, the Complainant emailed the WCB employee and said:

> I'm not sure if the correct address is being used. I see on the digital file a memo from [first name of a WCB employee] dated May 3 but it has a really old address (from a previous wcb claim)
>
> My current address is [Complainant's current mailing address]

[8] On the same day, the WCB employee responded incorrectly as follows:

> Hi [First name of Complainant] – the updated file was sent to your email address – not home address. Please review your email. thank you.

[9] On November 22, 2024, the Complainant made a complaint to the WCB about the privacy concern with respect to the WCB sending mail with their private information to their former mailing address.

[10] On November 26, 2024, the Complainant sent a follow-up email to the WCB to clarify their current mailing address.

[11] On December 11, 2024, the WCB responded:

> Regarding your address, although some mail was returned from your old address, your current address is updated in our records. Any future documents being mailed will be sent to your new address.

[12] In an email dated December 24, 2024, the WCB responded to the Complainant and conceded that it would proactively report another privacy matter to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). The WCB proactively reported the other matter to this office on that same day. This Investigation Report has no connection to that matter whatsoever.

[13] On January 20, 2025, having reviewed material in connection with the other matter forwarded by WCB, the OIPC contacted the Complainant. In discussions with the Complainant, the OIPC learned about the Complainant's concern over WCB continuously sending mail to their former mailing address.

[14] The WCB confirmed to the OIPC that all letters it had sent to the Complainant's former mailing address were returned unopened and untampered, except for the last one dated May 3, 2024. In an email to the OIPC dated March 10, 2025, the WCB explained that because the letters were returned unopened and seemingly untampered, it did not consider this to be a privacy breach. The WCB could not confirm the return of the letter dated May 3, 2024.

[15] On April 14, 2025, the OIPC notified the WCB and the Complainant that an investigation would be commenced.

[16] On May 13, 2025, the WCB provided its submission to the OIPC.

[17] The Applicant had provided a submission to the OIPC on February 20, 2025, in relation to the other matter, which also contained a statement with respect to this matter.

III DISCUSSION OF THE ISSUES

1. Does the OIPC have jurisdiction?

a. Is FOIP engaged in this matter?

[18] The WCB is a "government institution" pursuant to subsection 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP) and section 3 and PART I of *The Freedom of Information and Protection of Privacy Regulations* (FOIP Regulations). As such, FOIP is engaged. The OIPC has jurisdiction under FOIP to undertake this investigation.

b. Is HIPA engaged in this matter?

[19] For *The Health Information Protection Act* (HIPA) to be engaged, three elements must be present: there must be a trustee, there must be personal health information, and the personal health information must be in the custody or control of the trustee.

[20] The WCB qualifies as a "trustee" pursuant to subsection 2(1)(t)(i) of HIPA.

[21] The mail in question with this investigation, as sent by the WCB, contained payment statements for health services provided to the Complainant. Such information qualifies as personal health information pursuant to subsection 2(1)(m)(ii) of HIPA, which provides as follows:

> **2**(1) In this Act:
>
> ...
> (m) "personal health information" means, with respect to an individual, whether living or deceased:
>
> …
> (ii) information with respect to any health service provided to the individual;

[22] Therefore, the personal health information of the Complainant that was in the custody and control of the WCB was sent, by the WCB, to the wrong address. As such, HIPA is engaged.

[23] The OIPC also has jurisdiction to undertake this investigation under the jurisdiction as afforded by HIPA.

[24] In the next section of this Investigation Report, subsection 24(1.2) of FOIP and subsection 4(4)(h) of HIPA will be addressed with respect to how they interact in the collection of information for the purposes of administering *The Workers' Compensation Act, 2013*.

2. Did privacy breaches occur?

[25] A privacy breach occurs when personal information and/or personal health information is collected, used and/or disclosed without authority under FOIP and/or HIPA. Privacy breaches can also occur when personal information and/or personal health information is not appropriately safeguarded pursuant to subsection 24.1 of FOIP section and section 16 of HIPA, or collected or used in a way that is not accurate nor complete as required by

section 27 of FOIP and section 19 of HIPA (see OIPC Investigation Report 103-2018, 105-2019, 106-2019 at paragraph [25]).

[26] To determine if privacy breaches occurred, the OIPC must first determine if personal information or personal health information is involved in the matter. If so, then the OIPC must determine if the personal information and/or personal health information was collected, used and/or disclosed without authority under FOIP and HIPA, resulting in privacy breaches.

a. Is personal information involved?

[27] Personal information is defined at subsection 24(1) of FOIP, though the list provided is not exhaustive. Personal information is information that is about an identifiable individual, and that is personal in nature. Information is *about* an identifiable individual if the individual can be identified from the information, a common example is if the information includes the name of the individual. Further, and in keeping with basic logic, information is personal in nature if it provides something identifiable about the individual (see OIPC Review Report 005-2025 at paragraph [33]).

[28] Based on a review of the mail that was intended for the Complainant, the mail contained information such as the Complainant's former mailing address, the complainant's work injury claim number, and payment statements for travel mileage and wage loss. These data elements can be defined by subsections 24(1)(d), (e), (j) and (k)(i) as follows:

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> ...
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> (e) the home or business address, home or business telephone number or fingerprints of the individual;
>
> ...

> (j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness;
>
> ...
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual;

[29] Therefore, this matter involves "personal information" as defined by subsection 24(1)(d), (e), (j) and (k)(i) of FOIP.

b. Is the personal health information in this matter also considered personal information under FOIP?

[30] In paragraphs [19] to [23] above, it was found that personal health information as defined by subsection 2(1)(m)(ii) of HIPA was sent to the wrong address by the WCB. As stated earlier, this analysis must consider how subsection 24(1.2) of FOIP and subsection 4(4)(h) of HIPA interact.

[31] Subsection 24(1.2) of FOIP provides that personal health information in the possession or under the control of the WCB is personal information under FOIP as follows:

> **24**(1.2) Personal health information in the possession or control of the Workers' Compensation Board is personal information for the purposes of this Act.

[32] This is because subsection 4(4)(h) of HIPA provides that PARTS II, IV and V of HIPA do not apply to personal health information collected for the purposes of *The Workers' Compensation Act, 2013*. Subsection 4(4)(h) of HIPA provides as follows:

> **4**(4) Subject to subsections (5) and (6), Parts II, IV and V of this Act do not apply to personal health information obtained for the purposes of:
>
> ...
> (h) *The Workers' Compensation Act, 2013*;

[33] Since the Complainant submitted the "Worker's Initial Report of Injury" dated September 8, 2023, to the WCB as part of their obligation as a worker pursuant to section 51 of *The Workers' Compensation Act, 2013*, the OIPC is mindful of the fact that PARTS II, IV and

V of HIPA do not apply to the personal health information at issue in this matter. However, PARTS I, III, VI, VII, VIII, and IX of HIPA are still relevant to this analysis and some of those PARTS will be discussed later in this Investigation Report.

c. Was the personal information and personal health information collected, used and/or disclosed without authority under FOIP and HIPA, resulting in privacy breaches?

[34] It must now be determined if the Complainant's personal information and personal health information were collected, used or disclosed without authority under FOIP and HIPA. If so, then a privacy breach (or breaches) occurred.

[35] FOIP does not define the terms "collect" or "use". However, HIPA defines these terms as follows:

> **2**(1) In this Act:
>
> ...
> (b) **"collect"** means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means;
>
> …
> (u) **"use"** includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[36] Similarly, the OIPC considers that to "collect" personal information under FOIP means to gather, obtain access to, acquire, receive or obtain personal information from any source by any means. Further, to "use" personal information under FOIP includes reference to, or manipulation of, personal information by the government institution that has possession or control of the information but does not include disclosure to another entity.

[37] Neither FOIP nor HIPA defines the term "disclosure". The OIPC has defined "disclosure" as the sharing of personal information with a separate entity, not a division or branch of

the public body in possession or control of that record/information.[1] Similarly, to "disclose" personal health information under HIPA means to share personal health information with a separate entity, not a division or branch of the trustee organization with custody or control of the personal health information.

[38] In this case, the OIPC finds that the sending of mail by the WCB to an external entity constitutes a "disclosure". In this case, it was a disclosure of the Complainant's personal information/personal health information.

d. Did the WCB have authority under FOIP and/or HIPA to disclose the Complainant's personal information and personal health information?

[39] Government institutions must not disclose an individual's personal information unless that individual has consented to the disclosure pursuant to subsection 29(1) of FOIP, or if the disclosure without consent is authorized by the conditions that are outlined in subsection 29(2) or section 30 of FOIP. Obviously, the disclosure of personal information without authority under FOIP is a privacy breach.

[40] Similarly, trustees must not disclose an individual's personal health information unless the individual has consented to the disclosure pursuant to subsection 27(1) of HIPA, or if the disclosure without consent is authorized pursuant to the conditions as outlined in subsections 27(2), (3), (4), (5), (6) or sections 28 or 29 of HIPA. Once again, the disclosure of personal health information without authority under HIPA is a privacy breach.

[41] As already explained in paragraphs [30] to [32] of this Investigation Report, the interaction of subsection 4(4)(h) of HIPA and subsection 24(1.2) of FOIP lead to the obvious conclusion that the personal health information in this matter clearly falls under the jurisdiction of FOIP.

[1] At page 71 of *Saskatchewan Information and Privacy Commissioner 2007-2008 Annual Report*; and see paragraph [16] of OIPC Investigation Report 224-2024.

[42] To review the timeline once again, the WCB sent mail to the Complainant's former mailing address despite the Complainant having provided their current mailing address. The first time the Complainant provided their mailing address to the WCB was on the Complainant's "Worker's Initial Report of Injury" form dated September 8, 2023. However, the WCB sent mail to the Complainant's former mailing address on January 9, 2024, January 10, 2024, January 26, 2024 and on two occasions on February 5, 2024. Even after the Complainant provided their current mailing address a second time to the WCB on March 25, 2024, the WCB still sent mail to the wrong address on May 3, 2024.

[43] As explained in the background of this Investigation Report, the WCB's position is that the letters returned unopened and untampered did not constitute a privacy breach. However, the WCB conceded a privacy breach with respect to the unreturned letter of May 3, 2024. In its submission, the WCB explained as follows:

> This conclusion was based on information gathered at the time - including a review of the [Complainant's] claim file on Eclipse and discussions with the current and former team leads. They confirmed that while some returned correspondences were sent to the old address, the [Complainant's] address had been updated – and no further correspondence was sent to the old address. Copies of the returned mail were also provided to the worker on March 25, 2024 by [name of WCB employee]. When the [Complainant] raised concerns about the incorrect address on address on November 22, 2024, the address had already been updated - and no further correspondence was being sent to the old address.
>
> However, now having identified that the letter dated May 3, 2024 was sent to the old address and remains unreturned, our position is that this constitutes a privacy breach.

[44] In 2012, the OIPC released Investigation Report F-2012-004 with respect to a similar privacy breach on the part of the WCB. That investigation report found that the WCB mailed personal information and personal health information to unintended recipients on four separate occasions. In one of the incidents, the mail was returned to the WCB unopened. Nevertheless, the OIPC found that a privacy breach had occurred. In that investigation report, the Commissioner wrote:

> [64] I have defined privacy breach in my office's resource Glossary of Common Terms – The Health Information Protection Act (HIPA) as follows:

> **PRIVACY BREACH** happens when there is an unauthorized collection, use or disclosure of [personal health information], REGARDLESS OF WHETHER THE [PERSONAL HEALTH INFORMATION] ENDS UP IN A THIRD PARTY'S POSSESSION.
>
> [65] Although it appears that Complainant A's personal information and personal health information did not end up in the possession of a third party, the incident still constitutes a privacy breach.
>
> [Emphasis in original]

[45] The key consideration in these types of privacy breaches is that if the sender of the personal information and/or personal health information fails to have sufficient safeguards in place, if the items are returned unopened – a privacy breach has still occurred. This is because there are several other options that could happen in a situation such as this. For instance, the unintended recipient could have opened the mail, or they similarly could have thrown the mail into the garbage or onto the public street. Further, FOIP nor HIPA authorizes the disclosure of an individual's personal information or personal health information to an incorrect mailing address. Regardless of whether the mail containing the information is unopened or untampered with, a privacy breach occurred every time the WCB sends personal information or personal health information to the incorrect mailing address. Also, as WCB concedes, the May 3, 2024 letter is a clear privacy breach because it was sent to the wrong address and has never been found.

3. Did the WCB respond to the privacy breaches appropriately?

[46] Whether the government institution or trustee appropriately responds to a privacy breach and takes the correct steps in responding is informed by sections 6-7 and 7-7 of the OIPC's *Rules of Procedure*. The following considerations are relevant:

- Was the breach contained;
- Were the affected individuals notified;
- Was the breach investigated; and
- Were appropriate steps taken to prevent future breaches.

Containment of the Breach

[47] Upon learning that a privacy breach has occurred, steps should be taken to immediately contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; and
- Correcting weaknesses in physical security.[2]

[48] Privacy best practices state that a government institution should attempt to retrieve personal information or personal health information that has "gone astray."[3] In its submission, the WCB said that all letters were returned except one. The WCB did not expand on its efforts to recover the letter that was not returned. For example, the WCB could have contacted the recipient at the Complainant's former mailing address to inquire about the letter and to request that it be returned.

[49] There is a finding that the WCB, did not take fulsome steps to adequately contain the privacy breach.

Notification of Affected Individuals

[50] It is best practice for government institutions and trustees to inform affected individuals when their personal information and/or personal health information has been breached. This is an obvious and crucial step that invokes the principles of fairness. Affected individuals must know of the possible risks to which they have been subjected and they

[2] See OIPC Investigation Report 290-2024, 007-2025 at paragraph [21]; See also the OIPC's resources *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Trustees*.
[3] See OIPC Investigation Report F-2012-004 at paragraph [175].

must be informed so they can take any remedial steps they deem necessary to protect themselves.[4]

[51] In this case, the affected individual is the Complainant. This person discovered the privacy breaches and informed the WCB of its repeated error in sending mail to the incorrect mailing address. There is a finding that since the Complainant was the party that discovered the privacy breaches, the need to notify is not necessary in this case.

Investigation of the Privacy Breach

[52] When considering the reasons for the privacy breach, government institutions and trustees should reflect on the root causes of the breach. This is an important step in eradicating future breaches of a similar nature.[5]

[53] In its submission, the WCB explained that the root cause was "human error":

> The root cause was human error. After the worker submitted the claim with the current address, the registration & stat coding supervisor reviewed the submission to create a new claim file on Eclipse (WCB claim file management system). However, employee states that she mistook the current address for the old address already on Eclipse, because both addresses are near identical. The old address already on file, was provided by the worker as part of an old claim file.

[54] The OIPC reviewed the Complainant's current and former mailing addresses. The addresses are indeed nearly identical. However, the WCB does not explain why it continued to send mail to the incorrect mailing address even after the Complainant sent an email on March 25, 2024, and again on June 5, 2024, to the WCB to notify it of its error.

[55] The OIPC asked the WCB for a copy of its audit log from its claim file management system that demonstrated when the WCB updated the Complainant's mailing address. Based on a review of the audit log, the WCB updated the Complainant's mailing address on July 25,

[4] See OIPC Investigation Report 290-2024, 007-2025 at paragraph [24]; See also the OIPC's resources *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Trustees*.
[5] See OIPC Investigation Report 290-2024, 007-2025 at paragraph [33]; See also the OIPC's resources *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Trustees*.

2024. The WCB did not explain why it took so long for it to update the Complainant's mailing address. The WCB should have fixed its error when the Complainant notified the WCB of the correct address, first on September 8, 2023 and again on March 25, 2024 and finally once again on June 5, 2024. The error was not fixed until July 25, 2024. The error was not fixed until July 25, 2024. This raises the spectre of whether the WCB employees failed to follow policies on updating addresses in its claims file management system. Further, are there even adequate policies and procedures in place to ensure employees are complying with section 27 of FOIP and section 19 of HIPA respectively? Section 27 of FOIP provides:

> **27** A government institution shall ensure that personal information being used by the government institution for an administrative purpose is as accurate and complete as is reasonably possible.

[56] Similarly, section 19 of HIPA provides:

> **19** In collecting personal health information, a trustee must take reasonable steps to ensure that the information is accurate and complete.

[57] Also, subsection 24.1 of FOIP imposes a "duty to protect" personal information upon government institutions. Specifically, section 24.1 of FOIP requires government institutions to establish policies and procedures to maintain administrative, technical and physical safeguard as follows:

> **24.1** Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

[58] Section 16 of HIPA imposes the same duty upon trustees. Section 16 of HIPA provides:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[59] In the course of this investigation, the OIPC inquired about relevant policies and procedures from the WCB. The WCB provided the OIPC with a copy of two policies that it believed to be relevant. "Privacy of Information (POL 05/20217)" states that the purpose of the policy is to "establish guidelines for protecting privacy during the access, collection and release of information within the control of the Workers' Compensation Board." However, based on a review of the policy, it does not set out expectations or provide guidance to WCB employees to ensure that the personal information and personal health information being collected is as accurate and complete as reasonably possible pursuant to section 27 of FOIP and section 19 of HIPA.

[60] "Authority for Disclosure (PRO 06/2017)" was the second policy the OIPC was referred to by the WCB. The purpose of the policy is to "establish guidelines for disclosure of information, in writing, in person, by email and over the telephone." Clauses 4 to 16 of that policy outlines how employees should verify the *identities* of individuals seeking information in-person or over the telephone before disclosing information. This policy does not speak to the issue of whether accurate and complete information is obtained from the

individual prior to the disclosure of personal information. For example, in this matter, the WCB employee failed to verify that the Complainant's mailing address in Eclipse matched the address the Complainant provided on their application *and* in their emails. There is a finding that the lack of adequate administrative policies contributed to human error, the root cause of the privacy breaches here.

[61] The WCB has not met its "duty to protect" pursuant to subsection 24.1 of FOIP or section 16 of HIPA. It lacks adequate policies/procedures on how it expects its employees to meet the requirements of section 27 of FOIP and section 19 of HIPA.

Prevention of Future Breaches

[62] In responding to a privacy breach, it is essential to learn from the breach and then to implement measures to prevent future breaches from occurring. Possible prevention steps include strategies such as adding/enhancing safeguards, providing additional training, monitoring or auditing systems and users, and providing additional training.[6]

[63] In its submission, the WCB said it was reviewing its policies and procedures:

> WCB is currently reviewing its policies and procedures as part of ongoing privacy compliance improvements. No changes have been implemented yet, and timelines are being assessed as the key phases progress.

[64] Earlier in this Investigation Report, the OIPC found that the WCB had not met its "duty to protect" pursuant to section 24.1 of FOIP and section 16 of HIPA because the WCB lacked adequate policies and procedures regarding section 27 of FOIP and section 19 of HIPA. I recommend that within 30 days of issuance of this Investigation Report that the WCB develop policies and procedures that provide guidance to its employees on how to meet the requirements of section 27 of FOIP and section 19 of HIPA to verify and use accurate information. I also recommend that WCB deliver training to its employees once the policies and procedures are developed.

[6] See OIPC Investigation Report 290-2024, 007-2025 at paragraph [35]; See also the OIPC's resources *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Trustees*.

[65] Further, in its submission, the WCB also explained its "legacy system is currently being replaced – which includes implementing a new organizational operating and claim management system. This will automate several processes and reduce human error." However, the WCB was not specific as to how automating processes would reduce human error. Replacing the current legacy system with a new one still does not address the root causes of this privacy breach because the error was human – not that of a system. This investigation has revealed that employees need to exercise great care to ensure that the personal information and personal health information that is being collected and used is accurate and complete at all times. New addresses must be recorded or updated immediately when provided.

[66] At paragraph [8] of Investigation Report H-2014-001, the OIPC explained that the combination of automating tasks with the lack of care in inputting data may result in more privacy breaches, not fewer:

> Our observation is that quite apart from any particular technology, privacy risks will continue to exist. Faxing may be a particularly vulnerable and high-risk-to-privacy technology but as this Investigation Report documents, more sophisticated computer technology may well eliminate or at least minimize certain risks but may also create or expand new and other risks. **Auto-dialing and stored memory of contact information may mean that instead of one misdirected fax there may be hundreds all sent to the incorrect address because there was a lack of care in inputting data.** Many of the misdirected faxes discussed in this Investigation Report reflect inadequacies in policy, procedure, and training. **It would be a serious error to expect that inappropriate use or disclosure of personal health information will cease to be a problem for public confidence in our health care system once fax machines are displaced by more sophisticated computer equipment.**[7]
>
> [Emphasis added]

[67] The OIPC takes this opportunity to caution the WCB in assuming that automating processes will reduce human error. In this case, "human error" resulted in several pieces of the Complainant's mail being sent to the incorrect mailing address. Automating the task of mailing correspondence may result in the problem growing exponentially. Automation is

[7] See OIPC Investigation Report H-2014-001 at paragraph [254].

not always the panacea it is held out to be. The OIPC suggests that the WCB ensures it has adequate policies and procedures in place to prevent privacy breaches from human error as it replaces its legacy system with a new one.

[68] There will be a finding that the WCB has not implemented any action to prevent a similar privacy breach from occurring in the future.

IV FINDINGS

[69] The OIPC has jurisdiction to undertake this investigation.

[70] Six privacy breaches occurred every time the WCB sent the Complainant's personal information/personal health information to an incorrect mailing address.

[71] The WCB has made an unsatisfactory effort to contain the privacy breach.

[72] Since the Complainant was the party that discovered the privacy breaches, the need for WCB to notify is not necessary in this case.

[73] The WCB has not met its "duty to protect" personal information/personal health information pursuant to subsection 24.1 of FOIP and section 16 of HIPA, because it lacks adequate policies or procedures to guide its employees on how to meet the requirements of section 27 of FOIP and section 19 of HIPA. The lack of these administrative safeguards, or the root cause of the privacy breaches, led to repeated human error in this instance.

[74] The WCB has not implemented any action to prevent a similar privacy breach from occurring in the future.

V RECOMMENDATIONS

[75] I recommend that within 30 days of issuance of this Investigation Report, WCB make efforts to contact the recipient at the Complainant's former mailing address and request that they return the letter that the WCB has not yet recovered dated May 3, 2024.

[76] I recommend that the WCB develop policies and procedures within 30 days of issuance of this Investigation Report that provide guidance to its employees on how to meet the requirements of section 27 of FOIP and section 19 of HIPA to verify and use accurate information.

[77] I recommend that WCB deliver training to its employees once the policies and procedures are developed.

[78] I recommend that WCB send a written apology to the Complainant within 30 days of issuance of this Investigation Report for breaching their privacy repeatedly by sending mail to the incorrect mailing address.

Dated at Regina, in the Province of Saskatchewan, this 30th day of May, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner