Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 293-2024; 009-2025

Saskatchewan Workers' Compensation Board

August 5, 2025

Summary: The Saskatchewan Workers' Compensation Board (WCB) proactively reported a privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) after receiving a privacy breach complaint from the Complainant. The Complainant was concerned that a WCB employee, a Customer Care Facilitator (CCF), disclosed details of their WCB claim to their employer. The Complainant alleged this led to the employer successfully appealing their WCB claim. After hearing from WCB and upon being dissatisfied with the response, the Complainant contacted OIPC to request an investigation.

A privacy breach occurred when the CCF disclosed the Complainant's personal information to the employer (verbally and in writing). The Commissioner made several findings with respect to the investigation of the matter, including that WCB: 1) did not take sufficient action to contain the breach; 2) possessed a lack of adequate administrative policies and procedures that contributed to the unauthorized disclosure of the Complainant's personal information; 3) failed to adequately identify the full scope of the privacy breach; and 4) did not have an effective plan to prevent future similar breaches. The Commissioner made recommendations, all arising from the above findings, including the suggestion of future breach containment steps as well as the development of policies and training regarding the disclosure of personal information to prevent future breaches of this nature from occurring.

I BACKGROUND

[1] On December 4, 2023, a Customer Care Facilitator (CCF) with the Saskatchewan Workers' Compensation Board (WCB) received a telephone call from an employer regarding the status of an employee's (Complainant's) WCB claim. Based on the CCF's case notes, the employer expressed concerns regarding the legitimacy of the claim and inquired if there was medical information to support the claim. The CCF advised that WCB had medical information to support the claim and that the employee was seeking support from a therapist. The CCF advised that the claim was accepted as a cumulative claim and advised the employer that they could appeal the decision if they disagreed. The employer asked if the CCF would share the details of certain traumatic events that the Complainant had furnished within WCB file. The CCF then provided this information and again advised the employer of the right to appeal in the future.

[2] On November 22, 2024, WCB received the following complaint from the Complainant:

> My CCF [Name of WCB employee][1] gave my Employer [Name of Acting Area Director] examples of some traumatic events I have experienced in my career, which based on audit information, those are not to be disclosed to the employer for a cumulative stress injury (2022 Provincial Auditor of Saskatchewan Report). The employer used these in their appeal letter to attempt to disprove my psychological/cumulative stress injury. The Emloyer's appeal was accepted…

[3] On December 24, 2024, WCB responded to the Complainant advising that it conceded a privacy breach:

> I am writing to inform you of a privacy breach involving your personal information and to extend my apologies.
>
> **Description of the Breach:** During a phone conversation with your employer on December 04, 2023, your Customer Care Facilitator (CCF) disclosed examples of traumatic events you experienced in your career, as well as details

[1] The words in square brackets have been inserted by this office to preserve the identity of employees involved in this investigation.

> regarding your cumulative stress injury. This disclosure occurred within the context of investigating your claim and employer's appeal – and included details of traumatic workplace incidents and the cumulative mental health injury diagnosis associated with these incidents.
>
> It has been determined that this information should not have been shared without following the proper process outlined under Section 174 of the Workers' Compensation Act. Even though your employer would have likely had access to this same information through a formal file release request under Section 174 of the Workers' Compensation Act, they are still required to follow the outlined process.
>
> It is also noted that although the disclosure may lead to privacy concerns, your employer is a government institution bound by privacy obligations – which requires them to safeguard your personal information. Nonetheless, the following actions are being taken or have already been taken to address the situation:
>
> - The CCF has been instructed to contact your employer to remind them of their obligations under privacy laws – and the need to handle your information with confidentiality.
> - The breach will be reported to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).
> - The breach has been contained, and your personal information has not been disclosed any further.
> - Internal measures are being reviewed to prevent similar incidents in the future.
>
> You also have the right to submit a complaint to the Office of the Information and Privacy Commissioner (OIPC)…

[4] This office opened two separate files in respect of this matter. On December 24, 2024, WCB proactively reported this privacy breach to this office which resulted in File 293-2024. On January 3, 2025, the Complainant submitted a separate complaint to OIPC which resulted in File 009-2025.

[5] On January 23, 2024, OIPC emailed WCB and the Complainant a notice of an investigation. OIPC advised WCB of the complaint and that OIPC would likely issue an Investigation Report.

[6] On February 14, 2025, WCB provided OIPC with its completed *Privacy Breach Investigation Questionnaire* (Questionnaire)[2], and other relevant documentation. On February 20, 2025, the Complainant provided OIPC with their submission.

[7] On June 3, 2025, OIPC informed WCB that an Investigation Report would be issued.

II DISCUSSION OF THE ISSUES

1. Does OIPC have jurisdiction?

a. Is FOIP engaged in this matter?

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

b. Is HIPA engaged in this matter?

[9] For *The Health Information Protection Act*[4] (*HIPA*) to be engaged, three elements must be present: (1) personal health information, (2) a trustee, and (3) the personal health information is in the custody or control of the trustee.[5]

---

[2] See OIPC *Privacy Breach Investigation Questionnaire*: https://oipc.sk.ca/resources/resource-directory/privacy-breach-investigation-questionnaire/.

[3] *The Freedom of Information and Protection of Privacy Act,* SS 1990-91, c. F-22.01, as amended. *The Freedom of Information and Protection of Privacy Regulations,* c.F-22.01 Reg 1 (April 1, 1992), as amended.

[4] *The Health Information Protection Act,* SS 1990-91, c. H-0.021, as amended.

[10] WCB qualifies as a trustee pursuant to section 2(1)(t)(i) of *HIPA*. Section 2(1)(m)(i) of *HIPA* provides as follows:

> **2**(1) In this Act:
>
> …
> (m) **"personal health information"** means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;

[11] WCB described the information involved as: "detailed information about traumatic events experienced by the worker in their role. These details were tied to the worker's mental health assessment and diagnosis." As outlined earlier in this Investigation Report, the CCF's case notes details the conversation with an agent of the employer. The CCF conceded that they told an agent of the employer that the Complainant was seeking support from a therapist and listed several traumatic events that formed the basis of the Complainant's claim.

[12] Finally, WCB stated that the personal health information in its custody or control is collected as part of its mandate under *The Workers' Compensation Act, 2013*[6] (*WCA*). To have "custody" means that a trustee has physical possession of the records including a measure of control over them. To have "control" means having the authority to manage the records such as providing for their storage, restricting and regulating their use all within the exercise of a measure of control.[7] WCB stated it collects personal health information as part of its duty to manage compensation files for eligible injured workers. By virtue of

---

[5] See OIPC Investigation Report 193-2024, 043-2025 at paragraph [17].

[6] *The Workers' Compensation Act, 2013,* SS 2013, c.W-17.11, as amended.

[7] See OIPC Investigation Report 266-2024, 031-2025 at paragraph [14].

this process, WCB maintains it has custody and control of the claimant's personal health information.

[13] OIPC finds that *HIPA* is engaged and has jurisdiction to undertake this investigation under the jurisdiction as afforded by *HIPA*. In the next section of this Investigation Report, we will discuss the interaction between section 24(1.2) of *FOIP* and section 4(4)(h) of *HIPA.* These two sections interact in the collection, use and disclosure of a worker's information for the purposes of administering the *WCA*.

2. Did a privacy breach occur?

[14] 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/personal health information is not appropriately safeguarded pursuant to section 24.1 of *FOIP* and section 16 of *HIPA*.[8]

[15] To determine if a privacy breach has occurred, OIPC must first determine if personal information or personal health information is involved. If so, then OIPC must determine if the personal information and/or personal health information was collected, used and/or disclosed without authority under *FOIP* and/or *HIPA*.

a. FOIP has primary jurisdiction

[16] WCB proactively reported to OIPC that a CCF verbally shared the Complainant's *personal health information*, as defined by section 2(1)(m)(i) of *HIPA*, with the Complainant's employer. As stated earlier, this analysis must now consider how section 24(1.2) of *FOIP* and section 4 of *HIPA* interact. Section 24(1.2) of *FOIP* provides that personal health information in the possession or under the control of WCB is personal information under *FOIP* as follows:

[8] See OIPC Investigation Report 103-2018, 105-2019, 106-2019 at paragraph [25].

> **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.

[17] Section 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 *WCA*. The combined effect of sections 4(4)(h) and 4(6) of *HIPA* provide that *FOIP* has supremacy as the legislation in this case:

> **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*;
>
> …
> (6) *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act* apply to an enactment mentioned in subsection (4) unless the enactment or any provision of the enactment is exempted from the application of those Acts by those Acts or by regulations made pursuant to those Acts.

[18] The only part of *HIPA* that does apply in this matter is Part III and that is the duty of a trustee to protect the personal health information in its custody. This "duty to protect" mirrors the protection offered by the privacy provisions within *FOIP*. This matter involves the personal health information of the Complainant, but it is also clear that the statute of prime application in this matter is FOIP because of the interaction between the provisions of section 4 of *HIPA* and section 24(1.2) of *FOIP*. The obvious conclusion is that the personal health information in this matter is equivalent to personal information under *FOIP*.

b. The factual background leading to disclosure

[19] *FOIP* does not define the term "collect" or "use". However, *HIPA* and FOIP interact in this case and the definition section of *HIPA* is of assistance. Sections 2(1)(b) and (u) of *HIPA* provide 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.

[20] Neither *FOIP* nor *HIPA* defines the term "disclosure". 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.[9]

[21] WCB reported to this office that the privacy breach resulted from a verbal disclosure of personal information. The table below provides a factual accounting of the disclosure based on documentation provided to OIPC during the course of this investigation:

Date	Event that occurred
September 8, 2023	The Complainant submitted a Workers' Initial Report of Injury form to WCB alleging a psychological injury claim.
September 14, 2023	WCB sent a letter to the employer informing it of the Complainant's work-related injury claim and that a decision was pending.
December 4, 2023	During a telephone call with the employer, the CCF revealed that the Complainant's claim had been accepted as a "cumulative injury" claim. The CCF disclosed that the Complainant had been seeking support from a therapist since August of 2022 and listed the traumatic events as reported by the Complainant and connected to their employment. The CCF advised that the employer could appeal the decision.
December 4, 2023	The CCF emailed the employer to follow up writing: "the claim has been accepted as Cumulative injury…" and once again, the CCF listed the traumatic events as reported by the Complainant in connection to the claim. The CCF wrote in the email: "…you will be getting an email regarding

[9] See OIPC Investigation Report 083-2023 at paragraph [14]; see also *Saskatchewan Information and Privacy Commissioner 2007-2008 Annual Report* at page 71.

	claim acceptance and process to appeal the decision. Please feel free to appeal this decision in case you disagree with it."
December 8, 2023	WCB informed the employer by letter of its approval of the Complainant's claim.
January 3, 2024	The employer emailed the CCF indicating they planned to submit an appeal and requested a phone call to discuss.
January 4, 2024	In a telephone call originated by the employer to discuss the appeal process, the CCF directed them to information available online. The CCF's notes reveal that the employer informed the CCF of their disbelief with respect to one of the disclosed traumatic events. The CCF advised the employer that this could be disputed upon appeal.
January 23, 2024	The employer notified the CCF and WCB of a formal request to appeal the WCB decision.
March 26, 2024	A WCB Appeals Officer issued a decision regarding the employer's appeal. The decision noted that the Complainant provided an additional statement in response to the employer's appeal submission. The decision concluded that "the employer's appeal is accepted, [the Complainant] does not have an acceptable workplace psychological injury claim… the original decision by the operations department to accept the claim will be reversed and the claim will be disallowed." The decision directed the Complainant of the right to appeal to the Board Appeal Tribunal if they wished.
November 22, 2024	The Complainant submitted a privacy breach complaint to WCB.
November 26, 2024	WCB emailed the Complainant requesting relevant claim number(s). The Complainant responded the same day providing same.
December 11, 2024	WCB emailed the Complainant requesting "more clarification regarding the specific information shared – as well as when and through what method it was shared." The Complainant responded on the same day providing a screenshot of the CCF's December 4, 2023 case notes of the verbal disclosure of their personal information to their employer.
December 24, 2024	WCB emailed the Complainant confirming a privacy breach on its part.

December 24, 2024	WCB proactively reported the privacy breach to OIPC.
January 3, 2025	The Complainant submitted a privacy breach complaint to OIPC.
January 13, 2025	The Complainant inquired with WCB as to how the appeal decision of their claim can be "upheld or viewed as unbiased given the privacy breach."
January 16, 2025	WCB emailed the Complainant stating: "Regarding the impact of your privacy concerns on your claim, the appeal decision acknowledges that the incidents referenced by your employer provided some context. However, it also states that this information had very little influence on the final decision."
January 22, 2025	The CCF emailed a letter to the Complainant's employer advising that personal information shared during their December 4, 2023, telephone conversation constituted a privacy breach. The letter stated that "the personal information in question related to specific traumatic events the worker identified as continuing to their cumulative mental health injury." In this letter, the CCF listed the traumatic events a second time. The CCF also noted that "ideally, this information should have been provided through a formal file release request under Section 174 of the Workers' Compensation Act." (It must be noted that the employer never filed a section 174 *WCA* release for the personal information in this matter.)

[22] WCB has only ever conceded the December 4, 2023, verbal disclosure of the Complainant's personal information. The documentation submitted by WCB to this office, as summarized in the table above, reveals that on December 4, 2023, the Complainant's personal information was disclosed in writing to the employer via an email and again by letter on January 22, 2025.

[23] Government institutions must be careful to only collect, use and disclose personal information in accordance with the provisions of *FOIP*. Needless to say, the collection, use and/or disclosure of personal information without authority under *FOIP* is a privacy breach. Section 29(1) of *FOIP* provides the following regarding the disclosure of personal information:

> **29**(1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 30.

[24] WCB concedes that its employee shared the Complainant's personal information "without proper authority". Their submission outlined that the only proper method of disclosure of this information would be if the provisions of section 174 of the WCA were to be invoked by the employer:

> Section 29 of the Freedom of Information and Protection of Privacy Act (FOIP) specifies circumstances under which an individual's personal information may be disclosed without their consent. In this case, the disclosure was unauthorized because sharing personal information with an employer for the purpose of appealing a WCB decision regarding a worker's injury, must adhere to the process outlined in section 174 of the Workers' Compensation Act. However instead of following the formal file release process, the CCF disclosed this information during a phone conversation.
>
> [Emphasis added]

[25] Section 174 of *WCA* mandates a formal written request from an employer requesting a reconsideration or application for a review of a decision with respect to a claim. Section 174 of *WCA* states as follows:

> **174**(1) In this section, **"employer's representative"** means a person authorized in writing by an employer to represent that employer.
>
> (2) If an employer has requested a reconsideration of or applied for a review of a decision made pursuant to this Act with respect to a worker's claim for compensation, notwithstanding that the employer is not a party to the reconsideration or review, the board may on written request, in accordance with this section, grant the employer or the employer's representative access to the information that the board used to make its decision with respect to:
>
> (a) the facts of the situation in which the injury occurred; or
>
> (b) the percentage of the cost of compensation that has been assigned by the board to the injury cost record of that employer with respect to the injury of the worker arising out of and in the course of the worker's employment with the employer.

> (3) The person receiving the information pursuant to subsection (2) shall use that information only for the purposes of the reconsideration or review.
>
> (4) If a request is made pursuant to subsection (2), the board shall:
>
> (a) serve written notice on the worker or the worker's representative of the request and of the information that it will grant access to; and
>
> (b) inform the worker or the worker's representative that an objection may be made to the release of the information within the period specified in the notice.
>
> (5) On the expiration of the period mentioned in clause (4)(b), the board shall, after consideration of any objections:
>
> (a) decide what information it will grant the employer or the employer's representative access to; and
>
> (b) serve written notice on the worker or the worker's representative of all information it has granted an employer or employer's representative access to.
>
> (6) The board shall not grant the employer or the employer's representative access to any information until the expiration of the period mentioned in clause (4)(b).
>
> (7) An employer may request the board to reconsider its decision with respect to the information the board has granted access to within 15 business days after the date of that decision.
>
> [Emphasis added]

[26] No formal section 174 of *WCA* request was initiated by the employer at the time of the CCF's verbal disclosure of the Complainant's personal information. In fact, the employer *never* submitted a formal file release request to WCB for this information.

[27] The position of WCB is that the employer *probably* would have had access to the same information had they followed the formal file release request under section 174 of *WCA*. It submitted that "this disclosure circumvented appropriate processes and exposed the worker's information prematurely, creating privacy risks, including potential distress over procedural irregularities."

[28] It may very well be the case that the employer would have been provided with the information that the board used to make its decision with respect to the facts of the situation as alleged by the Complainant. Unfortunately, the position adopted by WCB completely ignores the fact that section 174 of *WCA* provides for a distinct element of procedural fairness in connection with the process. Section 174(4) of *WCA* allows for notice to the worker (the Complainant) and provides for a right to object within the period of time outlined in the notice. The process that occurred in this matter completely side-stepped all procedural fairness requirements that the Complainant had every right to expect. The argument that the employer would *probably* have received the same information in any event, reveals a certain disconnect with the procedural fairness that is sewn into the very provisions of section 174 of *WCA*.

[29] There is a finding that the actions of WCB in this matter resulted in a privacy breach.

3. Did WCB respond to the privacy breach appropriately?

[30] Determining the appropriateness of a government institution's response to a privacy breach involves several considerations. Whether the government institution appropriately responds to a privacy breach and takes proper corrective measures is informed by sections 6-7 and 7-7 of OIPC's *Rules of Procedure*. The following considerations include:

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

a) Containment of the Breach

[31] Upon learning that a privacy breach has occurred, government institutions should immediately take steps to contain the breach. Depending on the nature of the breach, this may include:[10]

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.
- Revoking access to personal information.
- Correcting weaknesses in physical security.

[32] OIPC applies a standard of reasonableness to assess the steps a government institution takes to contain a privacy breach. There needs to be some reassurance that the government institution has reduced the magnitude of the breach and the risk to affected individuals.[11] Containing the breach means to recover the personal information/personal health information or to stop the unauthorized practices when the government institution/trustee learns of the breach."[12]

[33] WCB determined no malice was involved in the breach and so the CCF was never denied access to the case management system.

[34] On January 22, 2025, WCB notified the Complainant's employer that their employee's verbal disclosure of the Complainant's personal information constituted a privacy breach. WCB reminded the Complainant's employer of their obligation to safeguard the

[10] See OIPC Investigation Report 290-2024, 007-2025 at paragraph [21]; see also OIPC resources *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Trustees*.

[11] See OIPC Investigation Report 197-2022, 215-2022 at paragraph [19].

[12] See OIPC Investigation Report 151-2017, 208-2017, 233-2017, 235-2017 at paragraph [20].

Complainant's personal information. WCB wrote to the Complainant's employer as follows:

> The personal information in question relates to specific events the worker identified as contributing to [Name of Complainant]'s cumulative health injury [events]. Ideally, this information should have been provided through a formal file release request under Section 174 of the Workers Compensation Act.
>
> While we understand that this information was used solely for an appeal on the worker's claim, please remember that you are obligated to maintain its confidentiality and not use it for any other purpose. As government institutions, we are also bound by privacy frameworks to safeguard such information.

[35] WCB submitted to this office that "…the employer limited its use to appealing a WCB decision – mitigating any further unauthorized use or onward disclosure" but it is unclear how this conclusion was reached. No documentation or evidence was supplied by WCB that would substantiate such a conclusion. The Complainant raised concerns that the unauthorized disclosure of their personal information could have reached an audience beyond the employer. Once again, the Complainant provided no evidence or documentation to substantiate this concern, but we recognize the validity of this fear.

[36] It appears that WCB focused its containment efforts solely on the verbal disclosure of the Complainant's personal information. However, as outlined in the table at paragraph [21], the CCF inappropriately disclosed the Complainant's health care information by writing in an email to the employer on December 4, 2023 and in a letter dated January 22, 2025. While it appears that WCB was attempting to contain the breach by means of the January 22, 2025 letter, it simply resulted in further exacerbating the privacy breach by re-stating the details of the personal information one more time.

[37] Best practice for containment upon breach is retrieval.[13] As WCB did not have authority to share what it did both verbally and in writing, it should have taken steps to retrieve that

[13] See OIPC Investigation Report F-2012-004 at paragraph [177].

information (e.g. notes of telephone conversation or the follow-up email/letter from the CCF to the employer). This did not happen.

[38] There will be a finding that WCB's attempts to contain the breach was insufficient in that WCB: 1) did not take steps to ensure that there was no dissemination by the employer of the Complainant's personal information; and 2) did not retrieve the personal information and/or request that the employer destroy it and verify its destruction.

[39] There will be a recommendation that, within 30 days of the issuance of this Investigation Report, WCB inquire of the Complainant's employer in order to ascertain that it has destroyed the personal information in question. If these records are still in the possession of the employer, WCB must request that the employer confirm their destruction or return them.

b) Notification to Affected Individuals

[40] 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 a crucial step that invokes the principles of fairness. Affected individuals must be informed of the possible risks so they can take any remedial steps they deem necessary to protect themselves.[14]

[41] Section 29.1 of *FOIP* requires government institutions to notify individuals when their personal information has been breached and when there is a real risk of significant harm for the affected individual as the result of a privacy breach.[15] Section 29.1 of *FOIP* states:

> **29.1** A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal

[14] *Supra*, footnote 10 at paragraph [24]; see also OIPC resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[15] See OIPC Investigation Report 129-2024 at paragraph [28].

> information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[42] In this case, there is only one affected individual - the Complainant. The Complainant discovered the breach and informed WCB. There is a finding that since the Complainant was the party that discovered the privacy breach, there is no need to notify. Regardless, the Complainant was provided with a response in the form of a notice that outlined clearly the nature of the breach and an apology for the breach. The Complainant was informed of the right to file a complaint with this office. In most privacy breaches, notification should also include a listing of the type of harm that may occur, save in cases like this where reputational damage is the obvious concern.

[43] In its internal investigation report, WCB acknowledged that a privacy breach of this nature could lead to "reputational harm or distress". The issue of the risk of significant harm was discounted. The submission included the following:

> Section 29.1 of FOIP notes that a government institution is only required to notify the individual whose privacy was breached if "it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual".
>
> For the reasons that follow, it is my opinion that this did not create a real risk of significant harm to the Worker:
>
> - While the disclosed information is highly sensitive and could lead to reputational harm or distress, the employer limited its use to appealing a WCB decision – mitigating any further unauthorized use or onward disclosure.
>
> - The employer would also have probably had authorized access to the same information, if they had initiated a file release request.
>
> [Emphasis added]

[44] We have spoken earlier of the concern that this response presents in that it is oblivious to the application of procedural fairness as required by section 174 of the *WCA*. But our concern with the response in the matter goes further. In this case, the Complainant alleged

that the disclosure has caused "emotional distress, professional embarrassment, shame", and has "negatively impacted" their psychological well-being and mental health. An admirable response in a case such as this could have included an acknowledgement of the possible damage to reputation or loss of employment or professional opportunities and an acknowledgement that the information was quickly retrieved and destroyed.

c) Investigation of the Privacy Breach

[45] The government institution should investigate the root cause of a privacy breach once it has taken steps to contain it and after the provision of notice to affected individuals. The investigation must address the incident on a systemic basis and include a root cause analysis. The institution must consider its duty to protect personal information as set out at section 24.1 of *FOIP*. Specifically, section 24.1 of *FOIP* requires that a government institution establish policies and procedures to maintain administrative, technical and physical safeguards:

> **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.

[46] Section 16 of *HIPA* imposes the same duty upon trustees to protect personal health information. Section 16 of *HIPA* (PART III) provides as follows:

> **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.

[47] In assessing the root cause of a privacy breach, the government institution must review existing safeguards and explore where deficiencies may lie so as to effect necessary changes. Safeguards can be administrative (e.g., policies, procedures, confidentiality statements on contracts), technical (e.g., access controls on electronic storage) or physical safeguards (e.g., locked cabinets or bins, locked doors, security cameras).

[48] At the conclusion of its investigation, the government institution should understand what occurred so it can develop a plan to prevent future breaches. Some key questions in arriving at the proper safeguards to put in place include:[16]

1. When and how did your organization learn of the privacy breach?
   - Has the privacy breach been contained?
   - What efforts has your organization made to contain the breach?
2. What occurred?
   - What type of breach occurred (e.g., collection, use, disclosure, accuracy, etc.)?

[16] *Supra*, footnote 7 at paragraph [66]; see also OIPC resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

- What personal information was involved in the privacy breach?
- When did the privacy breach occur? What are the timelines?
- Where did the privacy breach occur?

3. How did the privacy breach occur?

- Who was involved?
- What employees, if any, were involved with the privacy breach? What privacy training have they received?
- Who witnessed the privacy breach?
- What factors or circumstances contributed to the privacy breach?
- What is the root cause of the breach?

4. What is the applicable legislation and what specific sections are engaged?

5. What safeguards, policies, and procedures were in place at the time of the privacy breach?

6. Did the organization observe the duty to protect?

- Were the safeguards, policies, and procedures followed?
- If no safeguards, policies, or procedures were in place, why not?
- Were the individuals involved aware of the safeguards, policies, and procedures?

7. Who are the affected individuals?

- How many are there?
- What are the risks associated to a privacy breach involving this information (e.g., is the affected individual at risk for identity theft, credit card fraud, etc.)?
- Have affected individuals been notified of the privacy breach?

Inadequate Procedural and Policy Guidance for WCB Employees

[49] WCB indicated in its internal investigation report that the CCF failed to understand the nature of the privacy breach and how the disclosure of personal health information constituted a privacy breach. In spite of this, WCB warranted that the CCF was aware of, and had access to, all organizational policies on disclosure. The policies referred to were drafted specifically towards disclosure of information pursuant to section 174 of *WCA*.

[50] WCB supplied this office with information on its in-house policies and procedures:

> All policies are available on WCB's intranet available to all staff – and it is expected that employees review and consult policies as needed. In addition, our standard practice is to distribute all newly implemented or updated policies when they take effect, to all staff - or to management, who then share with their teams. There is currently no requirement for employees to acknowledge specific policies reviewed - or to do so, on a regular basis.
>
> [Emphasis added]

[51] WCB provided OIPC the following policies and procedures, that it believed were relevant to this investigation:

- *Code of Ethics and Professional Conduct – Acknowledgment and Agreement* (Code), which the CCF signed on December 12, 2022. The Code includes a section on confidentiality that emphasizes an employee's duty to protect the confidential information of WCB, its customers and its employees. The policy notes that the WCB cannot divulge any such information unless "expressly authorized to do so."

- *Privacy of Information (POL 05/20217)* (effective July 1, 2017), which states that the policy's purpose is to "establish guidelines for protecting privacy during the access, collection and release of information within the control of the Workers' Compensation Board." The policy adds that it is an offence for any WCB staff, pursuant to section 172 of *WCA*, to divulge information unless required or permitted pursuant to *WCA*.

- *Authority for Disclosure (PRO 06/2017)* (dated June 20, 2017). The purpose of this policy is to "establish guidelines for disclosure of information, in writing, in person, by email and over the telephone."

- *File Release to Employer* (undated flowchart) that guides employees through the recommended steps in the analysis of possible release of personal information pursuant to section 174 of *WCA*.

- *Fact Sheet: Disclosure of Claim File Information to Employers* (updated 02/24), which states "there are instances where certain information must be disclosed to a worker's employer…The WCB has a responsibility to explain its decisions to workers and employers. As such, disclosure of certain claim information is necessary so that the WCB can explain its decisions to employers." This document also outlines claim information that is generally withheld from disclosure.

- *Redacting Files: Employer's Request for a Worker's File* (updated 11/23), states "despite employers being permitted access to claim file documents, it is only permitted in accordance with the specific criteria detailed in Section

> 174 of the Act, and information disclosed by the WCB must otherwise comply with the provisions of *FOIP*."

[52] WCB's overarching policy *Authority for Disclosure (PRO 06/2017)*, in place at the time of the breach, provided the following guidance in general and with respect to section 174 of *WCA* applications:

> 9. Where staff receive telephone requests for information from workers, employers or their respective representatives, these may be transferred to the appropriate staff assigned to the claim or employer account in question.
>
> …
> 13.Certain information can never be provided on the telephone. For example, electronic banking information, social insurance number, or provincial health number.
>
> …
> Employers and Representatives
>
> 35. To request copies of claim documents, an employer must use an Employers Request for Photocopy of Relevant Records in File(s) form for each claim. No formal appeal is prerequisite, but the issue in dispute must be clearly identified and must concern a decision made on the claim or a pending appeal.
>
> …
> 37. Where the employer requests copies of claim documents:
> a. The decision maker (Claims Entitlement Specialist, Case Manager, etc.) will identify which documents are relevant to the decision in question. Copies are made only of those claim documents that are identified as relevant to the decision on the claim. Copies may be redacted to block out irrelevant information.
>
> b. After identification by the decision maker, the selected copies will be compiled by Operations staff. These will be provided to the worker by the means described in Point 37, along with a letter of initial notification that they have 15 business days from receipt of the letter to request a reconsideration of the copies to be provided to the employer. Any objections raised by the worker must be related to specific documents and be provided in writing with reasons given.
>
> [Emphasis added]

[53] The *Authority for Disclosure* policy provides employees with guidance on the process outlined in section 174 of *WCA* when an employer requests copies of claim documents, but

clause 13 above is silent with respect to verbal and written requests from an employer with respect to personal information. The root cause of the privacy breach in this case is that the CCF did not fully comprehend that communicating personal information/personal health information verbally and in written form to an employer outside the procedural requirements of section 174 of the *WCA* was a violation of the "duty to protect" obligations entrenched in sections 24.1 of *FOIP* and 16 of *HIPA*. There is a finding that the lack of adequate administrative policies contributed to human error in this case.

[54] There will be a recommendation that, within 90 days of the issuance of this Investigation Report, WCB develop additional guidance for its employees with respect to the *Authority for Disclosure* policy involving disclosures of personal information pursuant to section 174 of *WCA* during the case management of a WCB claim.

Inadequate Investigation at the Appeal Level

[55] In 2022 WCB's processes in administering compensation claims for psychological injury were subject to a performance audit by the Office of the Provincial Auditor of Saskatchewan. The audit found that WCB needed to "set formal guidance on what key information is needed for appeals; what to communicate for appeal outcomes; and what claim information to release to employers for appeals." These conclusions were drafted with the hope of minimizing delays in the receipt of appropriate mental health support for injured workers and to assist in their return to work. In 2022 obvious inadequacies were evident in WCB process with respect to psychological claims of injury and the appeal process.[17]

[56] WCB policy *Appeals – Claims (POL 21/2013)* (effective date: January 1, 2024), provides:

[17] *Report of the Provincial Auditor to the Legislative Assembly of Saskatchewan: 2022 Report – Volume 1* at pages 3 – 4.

> 4. Access to the claim file is in accordance with the provisions of section 173 and 174 respectively and will follow the process outlined under PRO 06/2017, Authority for Disclosure.
> …
> 7. The decision will be made in accordance with the Act, policies and the rules of natural justice, which require the decision maker to:
>
> a. Act properly, fairly and without bias.
> b. Provide an opportunity for each party to state their case.
> c. Inform each party of the case that they must respond to.
> d. Consider all of the evidence.
> e. Ensure that the decision is made by those who consider the evidence, and
> f. Provide the parties with meaningful and timely reasons.

[57] When the Complainant inquired about how the appeal decision on their claim would be affected by the admission of a privacy breach, they were told by email on January 16, 2025 that it was likely that the information that was the subject of the privacy breach had "very little influence on the final decision".

[58] The WCB response to the Complainant did not adequately address the Complainant's obvious concerns about the procedural unfairness that resulted from the unauthorized sharing of their personal information in the period leading to the employer's filing of an appeal. WCB also failed to fully acknowledge the full scope of the privacy breach in only identifying a single unauthorized verbal disclosure of personal information. There will be a finding that the WCB investigation failed to fully identify the full scope of the privacy breach. There will be a recommendation that, within 60 days of the issuance of this Investigation Report, WCB develop an internal investigation protocol.

d) Prevention of Future Breaches

[59] Measures for the prevention of future breaches can include: adding/enhancing safeguards, providing additional training, and the regular monitoring/auditing of systems and system users.[18] The following considerations are relevant:[19]

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

[60] This office was informed by WCB in its formal submission that the employee involved in this incident was advised of the privacy breach and reminded to follow the file release process set out in section 174 of *WCA*. This constitutes an important step towards the prevention of future breaches. We also commend WCB for its proactive report to this office and in offering to provide additional privacy training to the CCF. However, the training was estimated to occur within the next six months. Waiting up to six months to provide privacy training to an employee who clearly misunderstands the statutory privacy laws is not timely. To be relevant and to ensure accordance with the province's privacy law, the re-training of this employee should occur as soon after the breach as possible. There will be a recommendation that, within 30 days of the issuance of this Investigation Report, WCB provide the CCF with remedial privacy training that includes a focus on the disclosure of personal information and processes employees are required to follow prior to such disclosure.

[18] *Supra*, footnote 10 at paragraph [35]; see also OIPC resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[19] *Supra*, footnote 9 at paragraph [35]; see also OIPC resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[61] WCB also provided the following details about measures it intends to implement to prevent future privacy breaches of this nature:

> WCB will develop a training module that focuses on the proper collection, use and disclosure of personal and health information under FOIP – as well as file release requests under section 174, WCA. Policies and procedural updates are also under review as part of ongoing privacy compliance improvements.
>
> WCB is currently reviewing its policies and procedures as part of ongoing privacy compliance improvements…
> WCB will enhance safeguards by developing targeted privacy and process-specific training.
>
> WCB plans to implement privacy training focused on permissible disclosures over the phone and within work injury investigations to mitigate the risk of similar breaches
>
> No specific practices have been identified for discontinuation at this time. However, we continue to assess our collection, use and disclosure processes to ensure compliance and mitigate risks.

[62] In paragraph [50] of this report, WCB conceded that it does not require its employees to acknowledge that they have reviewed and understood the relevant in-house privacy policies. There will be a recommendation that since WCB intends to review its privacy policies and procedures in the future, it consider measures to ensure: 1) policies and procedures are reviewed by staff on a regular ongoing basis; and 2) adequate training and procedural reminders are provided to staff.

[63] WCB noted that "at the time of the incident, annual mandatory privacy training was not mandatory." It noted that prior to October 2024, new employees, upon hire, completed privacy training provided by the Government of Saskatchewan. Since that time, WCB has implemented organization-specific training for all employees, which the CCF completed on October 16, 2024 (after the privacy breach occurred). WCB also indicated it plans to implement privacy training "focused on permissible disclosures over the phone and within work injury investigations to mitigate the risk of similar breaches."

[64] It is encouraging that WCB is turning its mind to developing such training because this office has previously identified gaps in WCB's training for its case management team in the past.[20] Still, WCB noted that "the focus is on developing a privacy refresher for all staff" and the timeline "for the broader initiative is approximately one year." When a privacy breach occurs, a government institution should take immediate steps to address gaps in its safeguards. There is a recommendation that, within 90 days of the issuance of this Investigation Report, WCB develop training to deliver to its employees that addresses the items outlined at paragraph [54] of this Investigation Report.

[65] There will be a finding that WCB has failed in its objective of future prevention of similar breaches.

III FINDINGS

[66] OIPC has jurisdiction to undertake this investigation.

[67] A privacy breach occurred as WCB disclosed the Complainant's personal information to the employer, verbally and in writing, without authority pursuant to *FOIP*.

[68] The WCB attempt to contain the breach was insufficient in that WCB: 1) did not take steps to ensure that there was no dissemination by the employer of the Complainant's personal information; and 2) did not retrieve the personal information or request that the employer destroy it and verify destruction.

[69] Since the Complainant was the party that discovered the privacy breach, the need to notify was not present in this case.

[70] The root cause of the privacy breach in this matter is that the CCF failed to understand that the communication of personal information/personal health information to an employer

[20] See OIPC Investigation Report F-2007-001 at paragraphs [201], [203] and [212].

outside the statutory requirements of section 174 *WCA* was a clear violation of the "duty to protect" principle. This principle is enshrined in section 24.1 of *FOIP* and section 16 of *HIPA*. The lack of WCB administrative policies that address this statutory duty contributed to the human error in this case.

[71] WCB failed to fully identify the scope of the privacy breach.

[72] WCB has failed in its objective of future prevention of similar breaches.

IV RECOMMENDATIONS

Re: Containment of the Breach

[73] There will be a recommendation that, within 30 days of the issuance of this Investigation Report, WCB inquire of the Complainant's employer in order to ascertain that it has destroyed the personal information in question. If these records are still in the possession of the employer, WCB must request that the employer confirm their destruction or return them to WCB.

Re: Investigation of the Privacy Breach

[74] I recommend that, within 90 days of the issuance of this Investigation Report, WCB develop additional guidance for its employees with respect to the *Authority for Disclosure* policy involving disclosures of personal information pursuant to section 174 *WCA* during the case management of a WCB claim

[75] I recommend that, within 60 days of the issuance of this Investigation Report, WCB develop an internal investigation protocol.

Re: Prevention of Future Similar Breaches

[76] I recommend that, within 30 days of the issuance of this Investigation Report, WCB provide the CCF with remedial privacy training that includes a focus on the disclosure of personal information and processes employees are required to follow before disclosing personal information.

[77] I recommend WCB consider measures to ensure: 1) policies and procedures are reviewed by staff on a regular ongoing basis; and 2) adequate training and procedural reminders are provided to staff.

[78] I recommend that, within 90 days of the issuance of this Investigation Report, WCB develop training to deliver to its employees that addresses the items outlined at paragraph [54] of this Investigation Report.

Dated at Regina, in the Province of Saskatchewan, this 5th day of August, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner