SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT F-2012-004

Saskatchewan Workers' Compensation Board

Summary: The Commissioner was notified of four separate incidents where Saskatchewan Workers' Compensation Board (WCB) mailed personal information and personal health information to unintended recipients resulting in unauthorized disclosures. He performed a systemic investigation into WCB's mail handling practices. WCB alleged that each incident was the result of human error. The Commissioner found that lack of clear and effective policies and procedures also contributed to three of the incidents. He also found that WCB did not track or monitor these breaches, nor did it deal with the breaches in a consistent and effective manner. He made a number of recommendations including one regarding the retrieval of personal information and personal health information that had gone astray.

Statutes Cited: *The Freedom of Information and Protection of Privacy Act,* S.S. 1990-91, c. F-22.01, ss. 2(1)(d), 24(1)(a), 24(1)(b), 24(1)(d), 24(1)(e), 24(1)(g), 24(1)(i), 24(2), 25, 29(1); *The Health Information Protection Act*, S.S. 1999, c. H-0.021 ss. 2(m), 2(m)(i), 2(m)(ii), 2(m)(v), 2(q), 2(t), 16; *The Workers' Compensation Act, 1979*, S.S. 1979, c. W-17.1, ss. 171.1 and 171.2.

Authorities Cited: Saskatchewan OIPC Review Reports F-2012-005, F-2012-002, F-2005-001; Saskatchewan OIPC Investigation Reports F-2007-001, F-2009-001, H-2007-001; Privacy Commissioner of Canada, *Incident Summary #1: Misdirected faxes containing health information end up in apartment managers' hands*; Alberta IPC Order P2012-02; Nova Scotia Freedom of Information and Protection of Privacy Review Office Review Report P-11-01.

Other Sources Cited: Saskatchewan OIPC: *Glossary of Common Terms: The Health Information Protection Act (HIPA), Helpful Tips: Privacy Breach Guidelines*; Ontario Ministry of Government Services, Information, Privacy and Archives Division, *FOI and Privacy Manual*; Access and Privacy Branch, Service Alberta, *FOIP Guidelines and Practices (2009)*, Saskatchewan Workers' Compensation Board: *Policy and Procedure Manual*: *Policy 10.1 and Procedure 10.5* and *Corporate Overview*.

I BACKGROUND

[1] My office had four files all dealing with issues involving the mail handling practices of the Saskatchewan Workers' Compensation Board (WCB). As such, I have combined all four into one systemic investigation report.

a) File 026/2009-FOI/BP (Incident #1)

[2] Complainant A provided my office with a letter from WCB to Complainant A dated November 21, 2008. The letter informed Complainant A of the following:

> Please find a copy of our letter dated November 5, 2008.
>
> This letter was returned to our office due to an error in your mailing address.

[3] My office notified WCB of our intention to undertake a breach of privacy investigation on March 10, 2009. We asked WCB to investigate the circumstances of the matter and specifically look into whether the letter in question was opened before it was returned.

[4] WCB responded in a letter dated March 17, 2009. It stated:

> With regards to the allegation that correspondence directed to [Complainant A] was sent to the wrong address, this is in fact correct. Correspondence dated November 5, 2008, from myself [the Privacy Officer] to [Complainant A] was addressed to 456 [name of street] when in fact her address is 425 [name of street].
>
> I have been advised by WCB mailroom staff that to the best of their knowledge the misaddressed letter was returned unopened to the Workers' Compensation Board.

b) File 233/2009-FOI/BP (Incident #2)

[5] Complainant B called my office on December 8, 2009 to inform us that he had found personal information of three individuals other than himself (Individuals #1, #2 and #3) among his own personal information sent to him by WCB.

[6] On December 10, 2009, Complainant B attended my office with the entire package sent to him by WCB.

[7] Complainant B's file information was sent to his home address via registered mail. The package was contained within two sealed envelopes inside the larger envelope. Both of these envelopes were sealed and labeled: *"This document is confidential and is to be opened only by the addressee."*

[8] My office copied 2 pages from Complainant B's file as follows:

- November 15, 2009 "Request For Copy of File" submitted by Complainant B to WCB; and
- November 24, 2009 letter from WCB to Complainant B advising that copies of the claim file were enclosed

[9] My office also retained the following document from Complainant B's package:

- A July 16, 2009 memo from the WCB Acting Manager of Appeals to a WCB CES III advising the following:

  > There is some documentation on this file, which does not belong. I believe this documentation was sent by the employer, [Business #1] of Regina. The documentation relates to a [Individual #1], [Individual #2] and [Individual #3]. Could you please ensure the documentation is removed from this file.

[10] My office also retained the documents containing the personal information of Individuals #1, #2 and #3 as follows:

- Documents containing information about Individuals #1 and #3 are single pages entitled "Hire/Profile" which contain usual human resources type information

about the individuals. These appear to be screenshots from the webpage powerpay.ca.

- The document containing information about Individual #2 is a "Status Change" form, also a screenshot from what appears to be the same webpage detailing information about the individual.

[11] In addition, there were a number of documents on Complainant B's file from Business #1 to WCB which my office did not retain, as they were not relevant.

[12] On December 15, 2009, my office wrote to WCB advising of the situation and requesting an investigation report be prepared if one did not already exist.

[13] On December 16, 2009, I received a copy of the WCB investigation report.

c) File 034/2010-FOI/BP (Incident #3)

[14] Complainant C called my office on May 26, 2010. He indicated that after requesting a copy of his own file from WCB, he received that of another individual (Individual #4). Complainant C indicated that he contacted WCB on May 21, 2010 and the person he spoke to admitted that WCB had sent his personal information to the wrong address.

[15] Complainant C brought the personal information of Individual #4 to our office that afternoon. It was sent to Complainant C by registered mail in a double sealed envelope.

[16] My office contacted the Privacy Officer of WCB that afternoon. He confirmed that Complainant C's personal information had been sent to Individual #4, and that it had been retrieved unopened from Individual #4.

[17] By letter dated July 13, 2010, my office advised WCB of our intention to investigate the incident. I received its investigation report on August 5, 2010.

d) File 089/2011-FOI/BP (Incident #4)

[18] On October 14, 2011, I received a letter from WCB proactively reporting a privacy breach. WCB noted that it had sent an Employer Cost Statement report (ECS) for a health region to another employer, a private business, (Business #2) on or near June 3, 2011. It advised that it was in the process of investigating the breach and informing the affected individuals. I applaud WCB for proactively reporting this incident.

[19] On October 18, 2011, I received WCB's investigation report. It appears 296 individuals were affected by this breach. The ECS contained the following personal information: employer name, work injury claim numbers, first initial and last name of workers, birthdates of workers and types of benefits workers have received for that month. WCB's report also indicates that this type of breach involving ECSs has occurred twice before in May 2008 and December 2007.

[20] On October 31, 2011, we received a letter from a Royal Canadian Mounted Police (RCMP) detachment. Attached to the letter was the ECS for the health region that had gone astray. Business #2 had given the personal information to the RCMP who then forwarded it to us for the purposes of this investigation.

[21] Within a month of being notified of the breach, my office received complaints from three of the affected individuals. I then took the decision to undertake a formal privacy breach investigation. My office advised WCB of such on November 8, 2011.

[22] My office sent WCB a complete analysis respecting all four matters with a list of recommendations on or about August 7, 2012. In reply, WCB indicated by letter dated September 11, 2012 that it would be taking measures to address three of our recommendations. WCB did not provide specifics as to how it would address the related concerns. WCB also indicated it would respond to the rest of the recommendations once I had issued this formal Report.

II ISSUES

1. Are *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act* engaged in these incidents?

2. Do Saskatchewan Workers' Compensation Board's policies and procedures properly define personal information and personal health information?

3. Did the misaddressed letter in Incident #1 result in a breach?

4. Was there an unauthorized collection of personal information in Incident #2?

5. What mailing practices contributed to the unauthorized disclosure of personal information in Incidents #2, #3 and #4?

6. Did Saskatchewan Workers' Compensation Board follow best practices when responding to these privacy breaches?

7. What are privacy best practices when retrieving errant personal information?

III DISCUSSION OF THE ISSUES

1. Are *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act* engaged in these incidents?

[23] To determine what privacy laws are engaged in these incidents, I must determine if WCB is a government institution or a trustee and if personal information or personal health information is involved in the incidents.

[24] WCB is both a "government institution" for the purposes *of The Freedom of Information and Protection of Privacy Act* (FOIP)[1] and a "trustee" for the purposes of *The Health Information Protection Act* (HIPA).[2]

[25] "Personal information" is defined in section 24 of FOIP. The relevant portions are reproduced 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:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
> …
>
> (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;
> …
>
> (g) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;
> …
>
> (i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;
> …
>
> (2) "Personal information" does not include information that discloses:

[1] *The Freedom of Information and Protection of Privacy Act,* S.S. 1990-91, c. F-22.01 at section 2(1)(d).
[2] *The Health Information Protection Act*, S.S. 1999, c. H-0.021 at section 2(t).

> (a) the classification, salary, discretionary benefits or employment responsibilities of an individual who is or was an officer or employee of a government institution or a member of the staff of a member of the Executive Council;[3]

[26] "Personal health information" is reproduced at section 2(m) of HIPA as follows:

> 2 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;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or
>
> (B) incidentally to the provision of health services to the individual; or
>
> (v) registration information;
>
> …
>
> (q) "registration information" means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;[4]

[27] This investigation is driven by section 29 of FOIP and section 16 of HIPA. Section 29 of FOIP prohibits government institutions from disclosing personal information without authority as follows:

> 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

[3] *Supra* note 1 at section 24.
[4] *Supra* note 2 at sections 2(m) and 2(q).

> individual to whom the information relates except in accordance with this section or section 30.[5]

[28] Section 16 of HIPA requires trustees to have written policies and procedures in place to protect unauthorized disclosure of personal health information.

> 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.[6]

a) Incident #1

[29] The material at issue in Incident #1 is a one page letter from WCB's Privacy Officer to Complainant A. The letter includes Complainant A's address which is personal information pursuant to section 24(1)(a) of FOIP. It also provides details of a letter sent to the Ministry of Advanced Education, Employment and Labour.[7] The WCB letter appears to be a reply to this letter. This would constitute personal information pursuant to section 24(1)(g) of FOIP.

[5] *Supra* note 1 at section 29.
[6] *Supra* note 2 at section 16.
[7] This Ministry has now been divided into the Ministry of Advanced Education and Ministry of Labour Relations and Workplace Safety.

[30] Also, WCB is a "no-fault system that protects employers and workers against the result of work injuries".[8] Simply by being a claimant of WCB would imply that the individual has acquired an injury which would constitute information about physical or mental health. As information about the physical or mental health of an individual is personal health information pursuant to section 2(m)(i) of HIPA, any record that identifies an individual as a claimant would be personal health information.

[31] The letter in question in Incident #1 identifies that Complainant A has an injury. Therefore some of the contents of the letter would also qualify as personal health information.

b) Incident #2

[32] The documents pertaining to three other individuals in which Complainant B found among documents sent to him by WCB also appear to contain personal information.

- The documents containing information about Individuals #1 and #3 are single pages entitled "Hire/Profile". These appear to be screenshots from the webpage powerpay.ca. The information contained in these documents are:
    1. A header which lists employees' identification number, name, pay type and pay rate;
    2. General information: consisting of employee number, first name, last name, middle initial, social insurance number (only recorded on Individual #1's form), street, city, province/state, country, postal/zip code, phone, email, and preferred language;
    3. Employee dates: birth date, hire date, last day worked, re-hire date;
    4. Compensation information: status (i.e. active/inactive), pay type, pay rate, annual earnings, standard hours per pay; and
    5. Taxation information: province of employment and federal tax exemption.

- The document containing personal information of Individual #2 is a "Status Change" form, also a screenshot from what appears to be the same webpage. This form contains the following information:

[8]Saskatchewan Workers' Compensation Board (hereinafter WCB) *Corporate Overview*, available at www.wcbsask.com/WCBPortalPage/book_about_wcb/page_about_sask_wcb.html?navigationAction=page_about_sask_wcb.

1. A header which lists employees identification number, name, pay type and pay rate;
2. Action to be taken regarding Individual #2's employment status; and
3. Last day worked.

[33] The information within these documents qualifies as personal information in a number of ways.

[34] The first documents contain the birthdates of Individuals #1 and #3. That would qualify as personal information as it is information about an individual's age pursuant to section 24(1)(a) of FOIP.

[35] Hire date, last day worked, re-hire date and action to be taken regarding Individual #2's employment status would all qualify as work history and therefore personal information pursuant to section 24(1)(b) of FOIP. I have also previously found that an employee number would constitute employment history as well.[9]

[36] Social insurance numbers qualify as personal information pursuant to section 24(1)(d) of FOIP. The individuals' addresses qualify as personal information pursuant to section 24(1)(e) of FOIP. The taxation information qualifies as personal information pursuant to section 24(1)(i) of FOIP.

[37] Finally, the pay type, pay rate, annual earnings, standard hours per pay would constitute personal information pursuant to section 24(1)(b) of FOIP because it is "information relating to a financial transaction in which the individual has been involved". It would not be exempt from the definition of personal information pursuant to section 24(2)(a) of FOIP as Business #1 is not a government institution or local authority.

c) Incident #3

[9]Saskatchewan Information and Privacy Commissioner (hereinafter SK OIPC) Review Report F-2005-001 at [18] to [22], available at www.oipc.sk.ca/reviews.htm.

[38] Complainant C requested a copy of his file from WCB and instead received that of Individual #4.

[39] The copy of Individual #4's WCB file contained data elements that would qualify as personal information under section 24(1) of FOIP such as address, age and employment information.

[40] The file also contained many medical records pertaining to Individual #4 such as radiology reports following MRI's and ultrasounds, doctors' reports and notes from physiotherapists, to name a few. This would all be information with respect to the "physical or mental health" or "any health service provided to the individual" and therefore personal health information pursuant to sections 2(m)(i) and 2(m)(ii) of HIPA.

[41] As well, Individual #4's health services number appears several times within the documents provided to Complainant C. This qualifies as personal health information pursuant to section 2(m)(v) and 2(q) of HIPA.

[42] I note that WCB has stated during this investigation that FOIP does not apply to the personal information due to the paramountcy provisions provided by sections 171.1 and 171.2 of *The Workers' Compensation Act, 1979* (WCA).[10]

[43] I have dealt with this paramountcy issue in many of my Reports.[11] It is my view that both FOIP and sections 171.1 and 171.2 of the WCA work together and are not in conflict with each other.

d) Incident #4

[10] *The Workers' Compensation Act, 1979*, S.S. 1979, c. W-17.1, sections 171.1 and 171.2.
[11] SK OIPC Review Reports F-2012-002 at [17] to [24] and F-2012-005 at [19] to [23] and Investigation Reports F-2007-001 at [16] to [176] and F-2009-001 at [19] to [53], available at www.oipc.sk.ca/reviews.htm.

[44] The ECS that WCB mistakenly sent to Business #2 contained the following data elements for 296 individuals: work injury claim numbers, first initial and last name, birthdates and types of benefits workers have received for that month.

[45] These data elements would all qualify as personal information pursuant to section 24(1) of FOIP. Furthermore, all of these individuals are identified as claimants of WCB and therefore the list would also qualify as personal health information for the reasons discussed above.

[46] As WCB is both a government institution and a trustee and both personal information and personal health information are in question, it appears that both FOIP and HIPA are engaged in these circumstances.

2. Do Saskatchewan Workers' Compensation Board's policies and procedures properly define personal information and personal health information?

[47] Personal information and personal health information are defined in FOIP and HIPA respectively. However, it does not appear that the relevant policies and procedures of WCB in place at the time of these incidents use these terms consistently or effectively. I have previously recommended in my Investigation Report F-2007-001: "That WCB revise all relevant policies and procedures to ensure they are harmonized with FOIP and HIPA."[12] Any subsequent efforts made by WCB are not evident or effective.

[48] It appears WCB treats some personal information/personal health information as more sensitive than others. Examples of this practice are as follows.

[49] The versions of WCB's procedure entitled *Release of Information – Claim Files* has separate procedures for a "File Release Process" and "Process for File Release Where Claim Has No Sensitive Information".[13] The procedure does not give a definition of

[12]SK OIPC Investigation Report F-2007-001 at [243], available at www.oipc.sk.ca/reviews.htm.
[13]WCB *Release of Information – Claim Files, July 9, 2007 – Version.*

sensitive information but references policy 12/2003. However, the current WCB *Policy and Procedure Manual* notes that *Privacy of Information* (POL 06/2008)[14] supersedes policy 12/2003. The current *Privacy of Information* policy does not contain a definition of sensitive information. During this investigation, my office received a revised version of the *Release of Information – Claim Files* procedure. It does not use the term sensitive information, however it was dated March 19, 2012 which indicated it was revised after all 4 incidents occurred.

[50] WCB also sent my office flow charts that outline the procedure noted above. They are entitled: *Claims requiring review by Case Management / Claims Entitlement Staff* and *Process for file release where claim has no sensitive information*.

[51] As such, I will assume the procedures and corresponding flow charts for mailing documents with "no sensitive information" in place at the time of the incidents means documents that have no personal information or personal health information.

[52] With respect to Incident #1, my office asked WCB if the misaddressed letter in question contained personal information or personal health information. It replied on October 8, 2009 "I can firstly advise that there is both personal and personal health information contained in most if not all WCB claim records." We then asked why WCB did not use more rigorous mailing practices as suggested in my Investigation Report F-2007-001 to mail the letter.[15] WCB replied in its letter of March 12, 2010 as follows: "On the other hand ordinary business correspondence is not normally rich with personal details nor does it contain third party information." I take this to mean that the letter in question qualifies as "ordinary business correspondence".

[53] WCB's privacy breach report for Incident #4 dated October 18, 2011 stated:

> Employer Cost Statements contain the following information:

[14]WCB *Policy and Procedure Manual*: *10.1, Privacy of Information (POL 06/2008)* at p. 2, available at www.wcbsask.com/WCBPortalWeb/ShowProperty?nodePath=/WCBRepository/pdfs/PolicyManual.
[15]SK OIPC Investigation Report F-2007-001 at [251], available at www.oipc.sk.ca/reviews.htm.

> - Employer name and address;
> - Employer WCB firm number;
> - Work injury claim numbers;
> - First initial and last name of workers (e.g., J. Smith);
> - Workers' dates of birth;
> - Types of benefits workers have received for the injury for that month (e.g., wage loss benefits, clothing allowance, drug expenses).
>
> The cost statements do not contain other personal information (e.g., S.I.N., Health Insurance numbers, banking information, G.S.T. numbers).
> …
> While the risk of harm to each individual is low the large volume of information that was disclosed is of concern.

[54] While I recognize that some elements of personal information/personal health information have different degrees of sensitivity than others, it is my view that it must all be sufficiently protected. It has been my approach to consistently use the definitions of these terms as outlined in FOIP and HIPA for the sake of clarity. It is not up to government institutions to determine what types of personal information and personal health information should be protected and which do not. All personal information and personal health information should be managed with care and caution.

[55] Commissioners from across Canada are consistent with this view. Most recently, the Nova Scotia Freedom of Information and Protection of Privacy Review Office found the following in Report P-11-01:

> 7. I find that the WCB has erred in making a distinction in the definition of personal information between business card only and inherently personal. Either information falls within the definition of personal information or it does not. The WCB is not able to divide personal information into classes, one that is entitled to privacy protection and one that is not.
>
> 8. Given the mandate and business of the WCB, I find the WCB should make it clear in its Privacy Policy that staff are to view all claim files and their contents as "sensitive information" and treat it accordingly. I also find that the WCB's policies and practices should reflect that ***privacy is a private matter*** and that the impact of the

> disclosure of personal information should be left for the individual to decide not the WCB.[16]

[56] Although WCB appears to have made some changes, its policies and procedures are not clear on the definition of personal information and personal health information. Moreover, they do not convey the message that it all must be protected. Policies and procedures that match the language of the statues would be clearer and more effective.

3. Did the misaddressed letter in Incident #1 result in a breach?

[57] In its letter of March 17, 2009, WCB confirmed that a letter to Complainant A was misaddressed and mailed. It also advised that the letter appeared to have been returned unopened to WCB.

[58] In a letter dated August 5, 2009, my office pressed for further information as follows:

> In terms of your investigation into the misdirected letter, it is fortunate that "to the best of their knowledge", the WCB mailroom staff reported that the misdirected letter was returned unopened. However, regardless if there has been a breach or not, a breach of privacy investigation is intended to identify the cause of the breach and bring about changes to policies and procedures so that potential breaches will not occur in the future.
> Furthermore, the Commissioner has already made recommendations regarding the mailing policies of the WCB. More specifically, I refer you to paragraphs 233-237 of Investigation Report F-2007-001 as follows:
> …
> Please broaden the scope of your investigation into this matter. Please also provide additional details as to how you investigated this matter including the names of the individuals interviewed and dates of the interviews, etc. In absence of a detailed response, we may consider conducting our own interviews. We will eventually provide details of your investigation to the Complainant so that she may regain confidence in term of WCB's handling of her personal information / personal health information.

[59] My office received a letter from WCB dated August 28, 2009. It stated:

[16]Nova Scotia Freedom of Information and Protection of Privacy Review Office Review Report P-11-01 at pp. 33 and 34, available at http://foipop.ns.ca.

> Regarding the "misdirected letter", I can advise I was the author of the letter and provided the incorrect address in the correspondence.
>
> The letter was dated November 5, 2008, and returned to our offices on or near November 18, 2008.
>
> After receiving notice of the alleged breach from your office in your correspondence of March 10, 2009, I interviewed the WCB's Information Handling Supervisor who advised me that to the best of his knowledge the correspondence of November 5, 2008, had been returned to the WCB unopened. It was his recollection that no unopened mail had been received by the WCB during the time period in question.
>
> I am confident that the letter was returned unopened and no breach occurred.

[60] My office requested more information from WCB in a letter dated October 5, 2009 as follows:

> Additionally, we are not yet satisfied with your investigation regarding the misdirected letter. Your response has caused us to ask the following questions. A more thorough investigation may have covered these questions.
>
> It appears [Claims Entitlement Specialist III], sent a letter to the Complainant dated November 21, 2008 informing of the misdirected letter and enclosed the original letter. Have you interviewed [Claims Entitlement Specialist III] about this matter? Did she send the letter in the original sealed envelope to the Complainant? If not, when she received the letter, had it been opened? Did you track the path of the letter from the mail room to [Claims Entitlement Specialist III] to see if any other staff had contact with the letter and recalls if the envelope had been opened? Please provide answers to these questions and expand the investigation if necessary.
> In our letter of August 5, 2009, we also reminded you of the Commissioner's recommendations on the mailing practices of the WCB set forward in report F-2007-001. Please provide an update of the WCB's status on implementing these recommendations and comment on whether they may have prevented this situation.

[61] Again, in response WCB answered in a letter dated October 8, 2009 as follows:

> [Claims Entitlement Specialist III], was not interviewed.
>
> Perhaps an explanation of the document handling process at the WCB will help you to understand why this would not have provided any greater insight into whether or not the letter to the complainant was in its original envelope:
>
> - Incoming mail, including returned correspondence, is received by the mail room staff;

- The incoming mail is sorted by size; and
- The mail is placed in a mail opening machine. If there are open letters prior to insertion in this device the mailroom staff would notice as opened mail would cause the opener to jam;
- Mailroom staff forward the mail to the Document Processing Department;
- In the Document Processing Department the individual documents are scanned to the WCB's electronic document system;
- The original is sent to secure off site storage and a scanned electronic image is forwarded to the appropriate staff member's work queue.

> All [Claims Entitlement Specialist III] would have received would have been an electronic version of the original letter sent to the complainant. No documentation would have been physically delivered to her and the only staff that would have seen the letter would have been the mailroom staff who opened it and the Document Processing staff who scanned it to the electronic record.
>
> I have done all the investigation necessary and have done my best to explain the process. To the best of my knowledge the letter in question was returned unopened and I have nothing further to offer.
>
> The normally accepted means of sending correspondence was carried out in this case. As a result of human error the incorrect address was affixed to the correspondence.
>
> I assume that your request for an update on WCB mailing practices is a reference to the recommendation contained in paragraph 251 of report F-2007-001, as this is the only recommendation that specifically addresses the WCB mail handling practices.
>
> The WCB did not take the Privacy Commissioner's recommendation to mean that all government correspondence will be sent in via express post and placed in a double envelope. In fact his recommendation was not related to such correspondence. There is a difference between WCB disclosure documents that have been collected during the course of file development, and the sending of single pieces of correspondence during the course of day-to-day business operations.

[62] My office wrote to WCB on March 1, 2010. We clarified that the recommendations in my Investigation Report F-2007-001[17] was meant to apply to all mail containing personal information. We asked the following:

> As the WCB does not view this recommendation as appropriate for guarding against such potential privacy breaches, please advise as to which strategies it will be employing to ensure that similar incidents do not happen in the future.

[17] *Supra* note 15.

[63] WCB responded March 12, 2010 as follows:

> The context of OIPC Investigation Report F-2007-001 was in reference to the disclosure of file copies to workers and/or employers under authority of sections 171.1 and 171.2 of *The Workers' Compensation Act, 1979*. It was only within this context that the WCB agreed to adopt the "double envelope" recommendation.
>
> The WCB agreed to provide special attention to the mailing of the file record since this record contains a large volume of sensitive information, much of which has been provided to the WCB by third parties or contains information about third parties. On the other hand ordinary business correspondence is not normally rich with personal details nor does it contain third party information.
>
> We would be happy to hear from you on best practice regarding the handling of ordinary business correspondence.

[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.[18]

[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.

[66] The incident appears to have occurred as a result of human error. WCB has not offered any strategies for minimizing such errors in the future.

[67] My office also asked WCB to comment on why the recommendations I made in my Investigation Report F-2007-001 were not put into practice. These recommendations are as follows:

[18]SK OIPC *Glossary of Common Terms – The Health Information Protection Act* (HIPA), available at www.oipc.sk.ca/resources.htm.

> [251] **That the WCB adopt a new procedure for sending personal information or personal health information** to claimants that would include the following features:
>
> • Claimants should always be given the opportunity to attend at a WCB office and, after providing proof of identity, be able to physically pick up a copy of their information. WCB should obtain an acknowledgement of receipt.
>
> • In the event that option is not attractive to a claimant:
>
> - For claimants who live in any city or town, the file should be sent by courier to the claimant.
> - For claimants living outside of a city or town, the material should be sent by express post such that there is a record of the envelope and an ability to trace that envelope in the event that it does not arrive as anticipated.
> - A double-envelope system should be utilized. This includes an outside envelope with the name and address of the claimant. This also includes an interior envelope with a bold notice to the effect: **THIS DOCUMENT IS CONFIDENTIAL AND IS TO BE OPENED ONLY BY THE ADDRESSEE.**[19]
>
> [emphasis added]

[68] WCB stated that it did not follow my recommendation of double sealed envelopes to mean all correspondence. WCB believes this recommendation is for disclosure documents, in other words, mailing a claim file of a claimant when requested.

[69] For the letter in question in Incident #1, the recommendations I made regarding the mailing of personal information would have provided extra protection to the letter in the event it had been delivered to the wrong addressee and opened.

[70] I note the recent Order from the Office of the Information and Privacy Commissioner (IPC) for Alberta P2012-02 considered a similar situation. It stated:

> [para 29] The fact that the Complainant's personal information was improperly disclosed does not automatically or necessarily mean that the Organization failed to make reasonable security arrangements to protect it. I have explained that I must determine what steps were reasonable for the Organization to take, bearing in mind all of the relevant facts and circumstances.[20]

[19] *Supra* note 15.
[20] Alberta Information and Privacy Commissioner Order P2012-02 at [29].

[71] This incident constituted a privacy breach. In addition, given the lack of clarity in the policies and procedures regarding the safe handling of personal information and personal health information and the failure of WCB to adopt past recommendations, I cannot conclude that WCB took reasonable steps to protect the personal information in this case.

4. Was there an unauthorized collection of personal information in Incident #2?

[72] As noted earlier, Complainant B received personal information of three individuals from WCB.

[73] We received a breach of privacy investigation report dated December 14, 2009 from WCB. WCB reported that Business #1 sent WCB information about Complainant B. WCB's investigation report stated: "The employer mistakenly included five pages in its submission that were unrelated to [Complainant B's] appeal and contained the personal information of three individuals." Business #1 appeared to have reused paper to print Complainant B's information as Individual #1, #2 and #3's personal information was on the back of some of the pages. This appears to have been an unsolicited collection of these three individuals on the part of WCB.

[74] I note that Business #1 appears to be a private business; therefore, this office has no jurisdiction to undertake an investigation into its practices.

[75] Section 25 of FOIP states:

> 25 No government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.[21]

[76] Two FOIP resources from both Alberta and Ontario discuss 'collection'. Alberta's *FOIP Guidelines and Practices (2009)* states:

[21] *Supra* note 1 at section 25.

> *Collection* occurs when a public body gathers, acquires, receives or obtains personal information. It includes the gathering of information through forms, interviews, questionnaires, surveys, polling, and video surveillance. There is no restriction on how the information is collected. The means of collection may be writing, audio or videotaping, electronic data entry or other means.
> …
>
> **Unsolicited Information**
> If a public body does not have specific authority to collect unsolicited personal information and the information is not necessary for an operating program or activity of that public body, it is not an authorized collection (see *IPC Order 98-002*). **The public body should adopt a policy of either returning the unsolicited information or destroying it in accordance with a transitory records schedule.**
>
> For example, when the Calgary Police Commission requested the names and positions of board members from the Calgary Police Association, the Association also sent the members' home addresses and telephone numbers. Since the Commission did not need this additional information, the investigating officer recommended that it be returned to the Association, and that the Commission adopt a policy that all unsolicited information be returned (*IPC Investigation Report 2000-IR-002*).
>
> In some cases, a public body might keep unsolicited personal information for a specified period of time before destroying it (e.g. unsolicited résumés). The public body should keep the unsolicited information separate from other files so that it will not be improperly used or disclosed.[22]
>
> [emphasis added]

[77] Ontario's *FOI and Privacy Manual* states:

> Authority to Collect
>
> s.38(2) FIPPA / s.28(2) MFIPPA
>
> This section sets out the conditions under which personal information may be collected. Personal information is collected when the institution actively acquires the information or invites an individual or others to send personal information to the institution. **An individual may submit personal information on his/her own initiative without the information being requested by the institution. Receipt of**

[22]Access and Privacy Branch, Service Alberta, *FOIP Guidelines and Practices* (2009) at p. 198, available at http://foip.alberta.ca/resources/guidelinespractices/pdf/chapter7.pdf.

> **this information is not considered a collection unless the institution keeps or uses the information.**[23]
>
> [emphasis added]

[78] WCB had not addressed if it had authority to collect the personal information in question, so we asked it to do so in our analysis of May 16, 2012. In its response of July 6, 2012, WCB stated:

> The information that was provided to the WCB by the Complainant's employer about the Complainant was printed, by the employer of Individuals #1, #2 and #3, on the reverse side of paper that contained the information of Individuals #1, #2 and #3. The WCB did not collect this information, it was mistakenly provided to the WCB by the employer. Therefore, your query regarding the WCB's authority to collect the personal information of Individuals #1, #2 and #3 does not make sense to me.

[79] WCB subsequently confirmed that it was an unsolicited collection of personal information of Individuals #1, #2 and #3. As noted above, a collection, although indirect and unintentional, still constitutes a collection for the purposes of FOIP and HIPA. As WCB does not appear to have had authority to collect this personal information, it should have returned or destroyed the personal information immediately.

[80] I then must examine why the destruction of the personal information did not take place. This can be accomplished by reviewing how WCB receives mail which was explained by WCB for the purposes of Incident #1.

[81] As noted above, in its response WCB explained the following in a letter dated October 8, 2009:

> Perhaps an explanation of the document handling process at the WCB will help you to understand why this would not have provided any greater insight into whether or not the letter to the complainant was in its original envelope:
>
> - Incoming mail, including returned correspondence, is received by the mail room staff;
> - The incoming mail is sorted by size; and

[23]Ontario Ministry of Government Services, Information Privacy and Archives Division *FOI and Privacy Manual*, available at www.accessandprivacy.gov.on.ca/english/manual/index.html.

- The mail is placed in a mail opening machine. If there are open letters prior to insertion in this device the mailroom staff would notice as opened mail would cause the opener to jam;
- Mailroom staff forward the mail to the Document Processing Department;
- In the Document Processing Department the individual documents are scanned to the WCB's electronic document system;
- The original is sent to secure off site storage and a scanned electronic image is forwarded to the appropriate staff member's work queue.

[82] There does not appear to be a person monitoring mail at the point of collection to ensure personal information is not being collected without authority. There appears to be no check point before mail is scanned in to the electronic system and originals sent to offsite storage.

[83] I have previously commented on WCB's collection practices in my Investigation Report F-2009-001. I recommended: "That WCB develop a policy to screen unsolicited personal opinion and information about claimants that is gratuitously disclosed to WCB and has not or cannot be corroborated."[24]

[84] It appears that at one time a WCB employee noticed the personal information of Individuals #1, #2 and #3. A memo dated July 16, 2009 from the WCB's Acting Manager of Appeals to a WCB CES III was found on Complainant B's file as follows:

> There is some documentation on this file, which does not belong. I believe this documentation was sent by the employer, [Business #1] of Regina. The documentation relates to a [Individual #1], [Individual #2] and [Individual #3]. Could you please ensure the documentation is removed from this file.

[85] However, it does not appear that this memo was acted upon. WCB's investigation report of December 14, 2009 noted:

> July 16, 2009
> [Name removed], Acting Manager Appeals forwards a memo to [name removed], CES III (cc'ed to [name removed], Supervisor CES III) advising that the above noted documentation relating to the third parties does not belong on the Complainant's file and should be removed.

[24]SK OIPC Investigation Report F-2009-001 at [112], available at www.oipc.sk.ca/reviews.htm.

> July 20, 2009
> [Another CES III] was providing vacation coverage for [name of original CES III removed] and in error closes the memo from [name of Acting Manager Appeals] without removing the third party information.

[86] It appears that two people were notified of the unauthorized collection of personal information, yet no one acted on the memo. It does not appear that WCB has investigated why the Supervisor CES III did not follow up on this matter.

[87] It appears that WCB has taken many appropriate steps in responding to this inappropriate collection. In its investigation report dated December 14, 2009, WCB stated:

> **Action Taken**:
> - Documents immediately removed from [Complainant B's] file;
> - Contacted [Complainant B] requesting that documents be returned to WCB. [Complainant B] refused WCB request;
> - Correspondence sent to [Business #1] notifying them of the error and apologizing;
> - Correspondence sent to [Individual #1] notifying him of the error and apologizing;
> - Continued efforts to verify current addresses of [Individuals #2 and #3].
> - Legal Services requested examination of original pre-scanned documents from storage.

[88] We note that Complainant B gave the documents noted above to my office. WCB's report also listed the following future actions it planned to take.

> **Immediate**
>
> Instruct Team Leader:
>
> - Continue efforts to obtain addresses of two workers who have not been notified of the breach;
> - Continue efforts to retrieve information from Complainant. Send letter via courier to Complainant demanding the return of the documents;
>
> **Future**
>
> - Ensure the existence of and enforcement of controls at the copy preparation stage to ensure that workers do not receive documents of other

workers, and/or third parties where the information of or from the third party is not relevant to the worker's claim;
- Use "claim copy" watermark paper for claim copy printing, preferably colour stock;
- Ongoing training and reinforcement of the documented mail and scanning, and document removal practices;
- Ongoing training and reinforcement of the documented file release practices.

[89] WCB had not indicated if it has gone to reasonable efforts to contact Individuals #2 and #3. We asked them to clarify in our analysis of May 16, 2012. In its response of July 6, 2012, it stated:

> Written correspondence was sent to Individuals #1, #2 and #3 in December 2009 advising them of what had occurred. No further steps were taken.

[90] Further, WCB's beach of privacy report dated December 14, 2009 states: "Legal Services requested examination of original pre-scanned documents from storage." It was unclear if the personal information of Individuals #1, #2 and #3 had been culled from the hard copy storage and destroyed. We asked WCB to clarify in our analysis of May 16, 2012. In its response of July 6, 2012, it stated: "These records would have been stored in a secured, offsite facility and have since been destroyed."

[91] Even though it was an unsolicited collection of personal information, WCB had no authority to collect it and failed to return or destroy it immediately or shortly after discovery. This constitutes a privacy breach. Further discussions of the disclosure of this personal information involved in Incident #2 will follow under the next issue.

5. What mailing practices contributed to the unauthorized disclosure of personal information in Incidents #2, #3 and #4?

[92] In each of the four incidents, WCB has indicated that the breaches were caused by human error. More specifically, for Incidents #2, #3 and #4, WCB stated:

> "WCB Privacy of Information Policy POL 06/2008) and Authority for Disclosure Procedure (PRO 04/2008) and existing practises for the release of claim record information were evident; the unauthorized disclosure was the result of human error – information not removed in July 2009, and prior to sending file to Complainant in November 2009." (WCB breach of privacy report for Incident #2, December 14, 2009)
>
> "As a result of human error a breach of privacy occurred when the personal and/or personal health information of [Complainant C] was mistakenly sent to another worker." (WCB breach of privacy report for Incident #3, June 4, 2010)
>
> "The cause of the breach was human error. Mail clerks failed to ensure that only the cost statement of [Business #2] was placed in the envelope destined for that employer." (WCB breach of privacy report for Incident #4, October 18, 2011)

[93] When human error is a factor in a breach time after time, it becomes necessary to re-examine any applicable policies and procedures to ensure they are clear, comprehensive and incorporate sufficient safeguards to reasonably prevent or reduce the likelihood of human error.

[94] WCB has a procedure for "*Release of Information – Claim Files*"; in other words, a procedure for mailing claim files that is derived from the suggestions from my Investigation Report F-2007-001[25] in which the material in question was a claim file. This procedure appeared to be engaged in both Incident #2 and Incident #3. WCB sent us two versions of this procedure. One was dated July 9, 2007 and was sent to our office with respect to Incident #2 on May 20, 2011. The other was dated May 20, 2007 and was sent with WCB's investigation report on August 3, 2010.

[95] The difference between the two versions of the *Release of Information – Claim Files* procedure sent to our office by WCB is as follows. The earlier version stated:

> **All copies of files released to clients, employers, their representatives/third parties must be done by way of a double envelope system. This process, if using a brown envelope, includes the name and address of the client on the outside envelope, and an interior envelope with a bold notice to the effect of "*This document is confidential and is to be opened only by the addressee*". If utilizing a**

[25] *Supra* note 15.

> **box to ship the documents, this same notice needs to be placed on the top of the documents in the box.**[26]

[96] In the later version, where the above paragraph had appeared, it stated:

> This document is confidential and is to be opened only by <name of person package is addressed to>[27]

[97] It is unclear if WCB sent the July 9, 2007 version of the *Release of Information – Claim Files* procedure in error or if the change between the May 20, 2007 version and the July 9, 2007 version was intentional. However, the change appeared to have been made more than three years before the first version was sent to our office. It is unclear which version WCB has distributed to its employees and follows as a corporation.

[98] In correspondence dated May 16, 2012, my office asked WCB to "[p]lease provide us with the most updated version of the *Release of Information – Claim Files* procedure document and confirm that it is the version currently used by WCB employees." WCB provided, with its submission of July 6, 2012, a version of March 19, 2012.

[99] It is unclear which version was being used by WCB at the time of these breaches; however, the latest version was created after each of these breaches occurred. We will base our recommendations on the current version of March 19, 2012.

[100] The document in question in Incident #4 was an ECS. It appears that the procedure for mailing this type of document is different from WCB's more specific *Release of Information – Claim Files* procedure. WCB's privacy breach report for Incident #4 dated October 18, 2011 stated:

> This breach which was similar in nature to those mentioned above which indicates that the current process for providing ECSs to employers is not adequate. I strongly recommend that a change in process be undertaken as indicated below.
> ...

[26] WCB *Release of Information – Claim Files - March 19, 2012 V2* at p. 1.
[27] *Supra* note 13.

- Change the process for delivering cost statements:
    - Double envelope the cost statements and send them via registered mail; or
    - Encrypt the documents and deliver via e-mail; or
    - Only make the statements available via the WCB secure on-line website.

[101] WCB did not provide a procedure for mailing ECSs, either old or updated, nor did it indicate which of the above listed options it actually planned to follow or a plan for implementing the decision.

[102] In my office's correspondence of May 16, 2012, we asked WCB if there is "a written procedure for the printing and distribution of ECSs? If so, please provide. What date was it implemented?"

[103] WCB's letter of July 6, 2012 included an attached procedure for mailing ECS dated January 25, 2012, that was put in to place after the Incident #4 occurred. However the letter stated:

> The following has been in place since 2004:
>
> **Generate Cost Statements:**
>
> a. In the cost statement screen, click on Generate Cost Statements. This will take about 5 – 10 minutes.
> b. Once the cost statements are generated, you must verify that they have been created properly.
>   i. Check about 12-15 firms to ensure the correct date, address, and the claim's costs and expenses were paid in that month. (As per [name of WCB employee] (IT), it is possible to see next months date due to timing.)
>   ii. Check the amounts at the bottom of cost statement screen to ensure correctness of arithmetic.
>   iii. Verify the totals – using a prior month's statement ensure the prior month's total is the same as the current months start.
>   iv. View the statement and ensure that they are created properly.
> c. Once cost statements have been generated and verified, send an e-mail to the ServiceDesk (in IT), Revenue Unit and Account Managers notifying them that the updates have been completed and the notices can be printed.

d. IT will bring the Cost Statements down when they are printed (this usually takes at least a day),
   i. Spot check to make sure the statements look okay
   ii. Remove WCB Cost Statement (#1108093) & give to HR – [name of WCB employee]
   iii. PDF the Federal Cost Statements (#0500003 + #0500062) and save in [name of internal WCB computer drive], then email Finance –([names of 3 WCB employees]), to advise the statements are ready.
   iv. Take to the mailroom for mail out.

[104] A general procedure for mailing personal information and personal health information would be simpler for staff to follow as opposed to having separate mailing procedures for each type of document mailed.

[105] In order to accept WCB's conclusions that each breach in Incident #2, #3 and #4 were solely the result of human error, I must compare the events that transpired as interpreted by WCB breach of privacy reports with the existing procedures.

a) Incident #2

[106] As noted in issue 4, one factor in this breach was the result of an unauthorized collection of personal information. A procedure for eliminating unnecessary collection of personal information and personal health information would have helped prevent this breach. It does not appear that WCB has such a procedure.

[107] However, there was also an inappropriate disclosure in this incident. The contents of Complainant B's file did not appear to have been reviewed before it was mailed to him. This resulted in an unauthorized disclosure of personal information of Individuals #1, #2 and #3 to Complainant B.

[108] I will compare the events as described in WCB's breach of privacy report for Incident #2 to the *Release of Information – Claim Files* procedure. I will use the May 30, 2007 version as it appears that it better incorporates my past recommendations on mailing personal information.

[109] WCB's breach of privacy report dated December 14, 2009 stated:

> November 15, 2009
> Complainant requests a copy of his claim record.
>
> November 24, 2009
> Claim record provided to Complainant by [name], Case Management Support without document review.

[110] The breach of privacy report does not give much detail as to how it was determined that the WCB employee listed above was responsible for "document review", so instead I look to the procedure for answers.

[111] The relevant steps of the May 30, 2007 version of the *Release of Information – Claim Files* procedure are as follows:

> **1.** On receipt of a completed worker's or employer's request for file release, Claims Entitlement or Case Management staff, having determined they require the file delivered to them, will utilize the following process:
>
> - An electronic request is made by the claim owner for Document Processing to copy the file. Document Processing will request a copy of the file from the high speed printer in our IT area. IT staff will print the file off, ensuring it is securely bundled with a goldenrod sheet on the top of each claim. The goldenrod sheets will have a form printed on them requiring the IT staff member printing the claim to initial, date and indicate the number of bundles per claim. These claims are then transferred to document processing. Please note, the goldenrod sheet remains with the bundles until it reaches the file owner.
> - Mail room staff picks up and delivers files to claim owners in Regina.
> - Saskatoon files are shipped to Saskatoon by courier within the normal mail delivery process.
>
> **2.**
>
> - Once the claim owner receives the file copy and has the opportunity to review the content, a letter to the client is created by the Admin Support staff member, and then delivered by the Admin Support staff member to the file owner.
>
> **PLEASE NOTE – The goldenrod sheet should never be removed from the file contents, and the owner should never provide the claim contents to the Admin Support staff. Claim contents should remain at the owner's desk until they are boxed/enveloped to be mailed.**

> - Once the letter is complete and the file contents are small enough to be put in an envelope, the envelope/label should be prepped and delivered to the owner's desk. The file contents should **never** be taken to [sic] the envelope. This same process should apply if the file is of a size that requires it to be boxed.

[112] Upon review of this procedure, several questions come to mind with respect to WCB's account of the incident. If the employee was responsible for reviewing the file, what was the review supposed to entail? Was the purpose of the review for checking for personal information of individuals other than the claimant in question? Did the employee know this? If such information was found, what was to be done with it? Were there procedures in place to remove such personal information from the electronic file or the offsite storage? Why is this not included in the *Release of Information – Claim Files* procedure? Was this employee familiar with this procedure document?

[113] Further, there appear to be other flaws in this portion of the procedure. First, the procedure appears to contradict itself when it states "Please note, the goldenrod sheet remains with the bundles until it reaches the file owner" and then states "**The goldenrod sheet should <u>never</u> be removed from the file contents…**". This does not appear to have been corrected in the March 19, 2012 version.

[114] In addition, the procedure states "The file contents should **never** be taken to [sic] the envelope." This appears to be a typo and should state "The file contents should never be taken out of the envelope." This may have been a factor in Incident #3 or #4. This does not appear to have been corrected in the March 19, 2012 version.

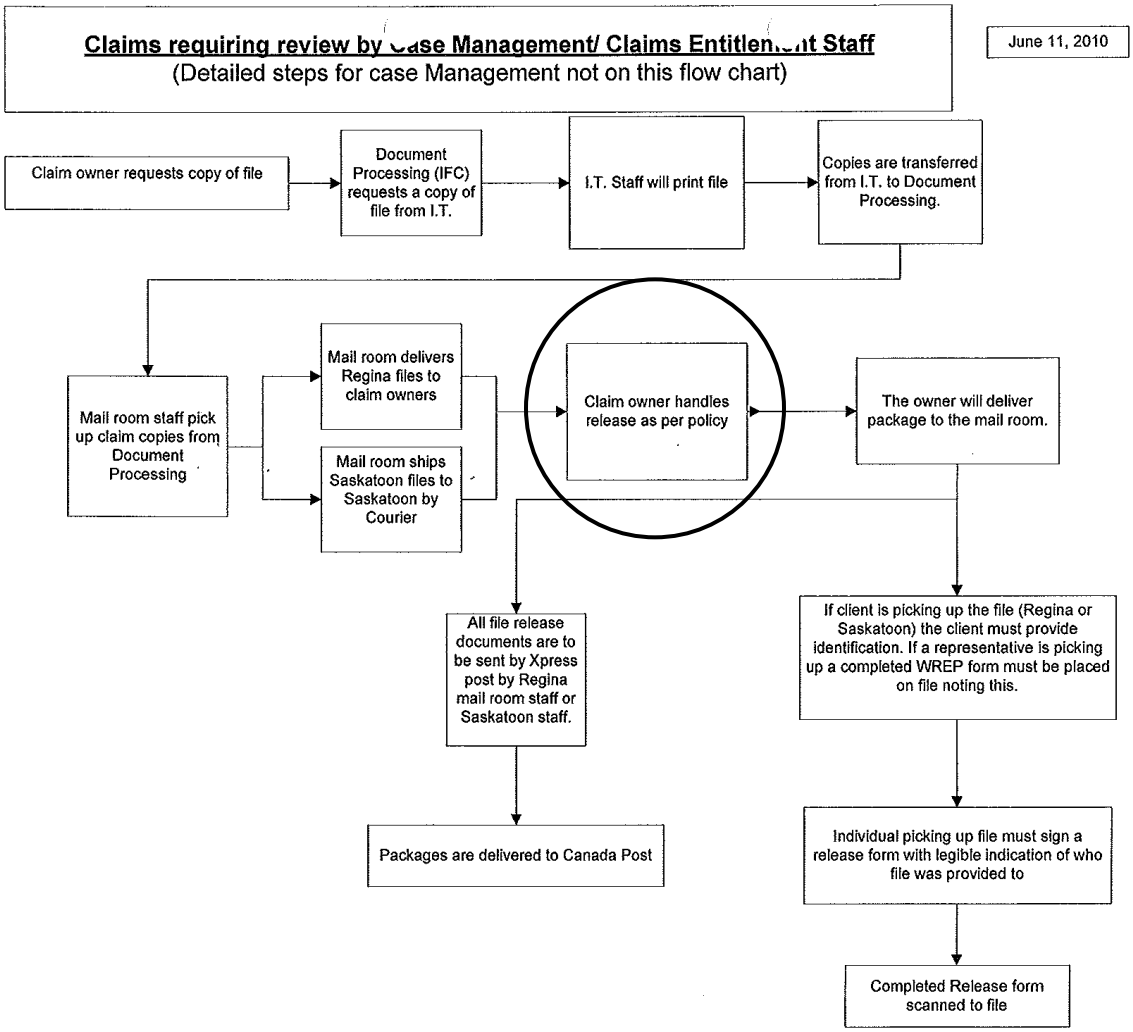
[115] In a letter dated August 31, 2010, WCB advised:

> I was advised in a memo dated March 20, 2010, from the WCB Director, Case Management South that training has been provided to staff regarding the controls required when preparing files to be forwarded to injured workers/employers. I was also advised that training has been provided to re-enforce the document and mail scanning document removal practices, and document file and release practices.

> Enclosed for your information are two flowcharts that are posted for staff to refer to to ensure that proper process regarding release of information under sections 171, 171.1 and/or 171.2 of *The Workers' Compensation Act, 1979* is being followed.

[116] WCB did not provide any details on the training that occurred. However, training using flawed material would not be effective.

[117] The following is an image of the aforementioned flow chart. It mirrors the *Release of Information – Claim Files* procedure. However, the flow chart provides no additional information critical for the review of a file as described above. At that junction (as circled), it simply refers to the procedure, which appears to be inadequate.



[emphasis added]

[118] In a letter of March 24, 2011, my office suggested that WCB's policy should have "explicit language regarding proper mail handling procedures including, but not limited to, the manual audit of double checking packages prior to releasing to the client."

[119] In response, WCB stated in its letter of May 17, 2011:

> Finally, your recommendation regarding WCB mail handling practices will be taken under consideration. Staff have been given instructions on the proper handling of information. They are professionals who deal with the collection, use and disclosure of personal and personal health information on a daily basis. For your information I am enclosing the instructions that are provided to staff [*Release of Information – Claim Files* procedure].

[120] In terms of Incident #2, the root cause was not human error. Instead, it does not appear that the *Release of Information – Claim Files* procedures are clear or specify why and how material needs to be reviewed before mailing. It is also uncertain which version of the WCB procedures is current and used within the organization.

b) Incident #3

[121] WCB's breach of privacy report for Incident #3 dated June 4, 2010 indicated that the *Release of Information – Claim Files* procedures "document outlines the process that staff are to follow when there is a request for release of the claim." As such the relevant steps will again be reproduced.

1. On receipt of a completed worker's or employer's request for file release, Claims Entitlement or Case Management staff, having determined they require the file delivered to them, will utilize the following process:

- An electronic request is made by the claim owner for Document Processing to copy the file. Document Processing will request a copy of the file from the high speed printer in our IT area. IT staff will print the file off, ensuring it is securely bundled with a goldenrod sheet on the top of each claim. The goldenrod sheets will have a form printed on them requiring the IT staff member printing the claim to initial, date and indicate the number of bundles per claim. These claims are then transferred to document processing. Please note, the goldenrod sheet remains with the bundles until it reaches the file owner.
- Mail room staff picks up and delivers files to claim owners in Regina.

- Saskatoon files are shipped to Saskatoon by courier within the normal mail delivery process.

2.

- Once the claim owner receives the file copy and has the opportunity to review the content, a letter to the client is created by the Admin Support staff member, and then delivered by the Admin Support staff member to the file owner.

  PLEASE NOTE – The goldenrod sheet should <u>never</u> be removed from the file contents, and the owner should <u>never</u> provide the claim contents to the Admin Support staff. Claim contents should remain at the owner's desk until they are boxed/enveloped to be mailed.

- Once the letter is complete and the file contents are small enough to be put in an envelope, the envelope/label should be prepped and delivered to the owner's desk. <u>**The file contents should never be taken to [sic] the envelope. This same process should apply if the file is of a size that requires it to be boxed.**</u>

****
All copies of files released to clients, employers, their representatives/third parties must be done by way of a double envelope system. This process, if using a brown envelope, includes the name and address of the client on the outside envelope, and an interior envelope with bold notice to the effect of "*This document is confidential and is to be opened only by the addressee*". If utilizing a box to ship the documents, this same notice needs to be placed on the top of the documents in the box.
****

- The claim owner and a co-worker (Admin Support, Case Manager, or other Case Management support, Team Leader, Payment person, etc.) will examine the goldenrod cover page to determine how many bundles are part of the complete file package.

- They will count the bundles, checking the first and last page of each bundle, to ensure that they show the worker's name and claim number. When they are satisfied that they do have the correct package, they will both sign the goldenrod sheet, where applicable and remove it from the pile.

- With both staff members present, the contents will be packaged into an envelope/box, and sealed. The owner will then deliver the package to the Mailroom, and the goldenrod sheet will be scanned to file.

[emphasis added]

[122] WCB's breach of privacy report for Incident #3 dated June 4, 2010 gives the following account of events:

> April 30, 2010
> [Complainant C] submits a Request for Copy of File (WROI) to the WCB.
>
> May 3, 2010
> [CES III] sends a CICS "activity" to [name], Document Processing Clerk requesting that a copy of the claim be sent to [Complainant C].
> [Document Processing Clerk] prints copy of [Complainant C's] file, attaches a cover letter and sends it to [Complainant C] via registered mail.
>
> …
> **Conclusion:**
>
> As a result of human error a breach of privacy occurred when the personal and/or personal health information of [Complainant C] was mistakenly sent to another worker.
> …
>
> In the case of [Complainant C] and the other worker [the Manager of Administrative Support] advised that the following process was followed:
>
> > "The requests to have these files printed and sent to the worker directly were both received on May 3. As part of the process, both requests were printed for our records. As both files were small the IFC person printed the files themselves.
> >
> > [Document Processing Clerk] printed the files and completed the RFIT sheet. Each file bundle was checked by [name of another unidentified WCB employee] and were placed in envelopes (as per the file release procedure).
> >
> > After reviewing the file and reviewing the IFC records I spoke with [Document Processing Clerk]. [Document Processing Clerk] indicated that she must have switched envelopes by accident when she sent them to the mailroom.
> >
> > [Document Processing Clerk] is fairly new to the IFC desk. On May 3 when this happened she was working on the IFC desk and was also trying to cover [a supervisor]'s duties as [the supervisor] was away. She feels badly that this mistake was made and understands the seriousness of the situation."
>
> It is not entirely clear from [CES III]'s CICS activity that the response to the request fell into that part of the Release of Information – Claim Files process entitled

> "Process for File Release Where Claim Has No Sensitive Information". She merely stated in her activity: "Pls send worker copy of his file."

[123] There are several points from WCB's privacy breach report that do not match up with the procedure.

[124] Firstly, the lack of definition of "sensitive information" as described in issue 2 clearly played a role in this breach. I do not see how employees would know which procedure to follow as there does not seem to be a mechanism to trigger one or the other. Regardless, as both the files printed on May 3, 2010 contained personal information and personal health information, the procedure for mailing sensitive information was definitely warranted. Again, WCB's March 19, 2012 version of the procedure appears to have been corrected as references to sensitive information have been removed.

[125] Secondly, WCB reported that on May 3, 2010 "[Document Processing Clerk] prints copy of [Complainant C's] file, attaches a cover letter and sends it to [Complainant C] via registered mail." However, according to the procedure, the Document Processing Clerk is supposed to print off the copy and send it to the claim owner for review. Then an Admin Support staff member is supposed to prepare a letter and give it to the claim owner. It appears from WCB's report that this portion of the procedure was bypassed.

[126] The procedure is unclear on who is supposed to prepare the envelope and who is supposed to place the material in the envelope. At one point, the procedure states: "The file contents should never be taken to [sic] the envelope." This sentence is unclear and unhelpful. The procedure then states:

- The claim owner and a co-worker (Admin Support, Case Manager, or other Case Management support, Team Leader, Payment person, etc.) will examine the goldenrod cover page to determine how many bundles are part of the complete file package.
  …
- …When they are satisfied that they do have the correct package, they will both sign the goldenrod sheet, where applicable and remove it from the pile.

- With both staff members present, the contents will be packaged into an envelope/box, and sealed. The owner will then deliver the package to the Mailroom, and the goldenrod sheet will be scanned to file.

[127] It does not appear that the claim owner was present when the packages were put into the envelope as required by the procedure.

[128] Goldenrod sheets appear to be a safeguard in the mailing process. At our request, WCB provided copies of the goldenrod sheets for Incidents #2 and #3. However, WCB did not offer any analysis on the role of the goldenrod sheets in these breaches or their effectiveness as a safeguard.

[129] It appears that the employees who prepared Complainant C's package did not follow the *Release of Information – Claim Files* procedure at all.

[130] Finally, the report states that the employee who did prepare Complainant C's file was new to the position. The report did not state whether this employee had been trained on this procedure and was prepared to act as supervisor for the day. Does the fact that her supervisor was not at work that day play a role in the breach?

[131] Although it was a factor, concluding that this breach was solely the result of human error was short-sighted. Clearly, the procedure for mailing claim file information was not followed in this case. In addition, the *Release of Information – Claim Files* procedure is not particularly helpful.

[132] The recommendations set forth in WCB's Breach of Privacy Report for Incident #3 are as follows:

Advise Manager, Administrative Support to:

- Create flow chart of the steps outlined in the "Release of Information – Claim Files" document and post it prominently for all staff to refer to;

- Immediately meet with staff to go over the process, and the flow chart and remind them of the importance of protecting the information in the WCB's care and control.

…

Advise Team Leaders to:

- Speak with staff about the importance of reviewing files for sensitive information prior to release to the worker, and if after such a review it has been determined that there is no such information on the file that the instructions to document processing to send the file state that there is no sensitive information.

[133] We assume the flow charts referred to in these recommendations are the same as those provided by WCB for the purposes of Incident #2.

[134] After review of WCB's privacy breach report and the *Release of Information – Claim Files* procedure, I have identified a few problems with these recommendations. One such problem is that an essential part of the flow chart references the procedure which appears to be inadequate as previously discussed.

[135] The recommendation to review the procedure with staff is ineffective as the procedure appears to be unclear, in addition to being inadequate.

[136] Finally, as discussed earlier, there does not appear to be a definition of "sensitive information" available to staff. Therefore, it may be futile to ask them to determine if a file contains "sensitive information" as per the final recommendation.

[137] More appropriate recommendations would be to revise the procedure to address all personal information and personal health information and to bring more clarity to the procedure. Staff should then be notified of the changes as part of privacy training.

[138] It is also significant to note that WCB wrote to Complainant C on June 15, 2010 responding to questions. The letter stated:

> As a result of unintentional error your claim was placed in the envelope addressed for another worker and visa versa. It is the responsibility of the individual who prints the claim to ensure that it is coupled together with the correct covering letter and placed in the correct envelope. Nothing more than unintentional error contributed to your situation.

[139] This statement does not appear to be consistent with the *Release of Information – Claim Files* procedure. It is the "claim owner" that is responsible for ensuring the file is paired with the covering letter. The procedure is unclear on who is responsible for stuffing the envelope.

c) Incident #4

[140] WCB's privacy breach report dated October 18, 2011 reported:

> June 3, 2011
> ECSs are printed by information technology and delivered to [name] Business Resource Specialist for review.
>
> June 6, 2011
> [Business Resource Specialist] delivered the ECSs to the mailroom for distribution. ECSs for the month of May 2011 are mailed to employers.
>
> …
>
> **Conclusion:**
> …
>
> The cause of the breach was human error. Mail clerks failed to ensure that only the cost statement of [Business #2] was placed in the envelope destined for that employer.

[141] WCB's report was deficient in explaining what actually occurred when the ECSs were mailed. Helpful information could have included:

- Who was responsible for preparing envelopes? Who is responsible for stuffing envelopes?
- Were there lists? Were the lists double checked?
- How were the ECSs bundled?
- Was there an envelope left over? Did the ECS for [Business #2] arrive at the correct destination?

- Was there a mechanism for double checking packages?
- The name of the health region that should have received the ECSs and [Business #2] start with letters that are not alphabetically sequential. Why would the two ECSs have been next to each other in a pile?

[142] Lack of detail suggests there was no written procedure for the mailing of ECSs. Such a procedure would have been helpful especially considering this same type of breach had happened at least twice before.

[143] It appears that a lack of written procedures including a system for double checking envelopes was a factor in this breach.

[144] Late in this investigation, WCB provided my office with a written procedure for mailing ECSs dated January 25, 2012, after Incident #4 occurred. The procedure in place for mailing personal information at the time of the incident did not specifically address ECSs.

[145] WCB's recommendations for Incident #4 as provided in its privacy breach report of October 18, 2011 were as follows:

> This breach which was similar in nature to those mentioned above which indicates that the current process for providing ECSs to employers is not adequate. I strongly recommend that a change in process be undertaken as indicated below.
> ...
>
> - Provide instruction to mailroom staff regarding the need to double check each cost statement to ensure that cost statements for one employer do not inadvertently get mailed to another, or included in the mailing to other employers.
> - Review privacy breach protocol with managers who can then review with staff…
> - Change the process for delivering cost statements:
> - Double envelope the cost statements and send them via registered mail; or
> - Encrypt the documents and deliver via e-mail; or
> - Only make the statements available via the WCB secure on-line website.
> - Change the content of the cost statements so that they do not contain any personal and/or personal health information about identifiable individuals.

[146] WCB did not indicate what course of action it intended to take.

[147] In a letter dated September 11, 2012, WCB indicated that the *Release of Information – Claim Files* procedure would be "corrected" but did not provide specific details on what would be changed.

[148] Although human error was identified by WCB as the cause of these privacy breaches, the lack of clear and consistent policies and procedures regarding the mailing of personal information and failure of WCB employees to follow the procedures, coupled with human error, is to blame for the disclosure related breaches in Incidents #2, #3 and #4.

6. Did Saskatchewan Workers' Compensation Board follow best practices when responding to these privacy breaches?

[149] Throughout the course of these four investigations we have either raised or noticed several concerns we have with the role of the privacy officer of WCB.

[150] A privacy officer is essential for both FOIP and HIPA compliance. This individual would be responsible for fostering a culture of privacy and have sufficient rank as to advise and influence senior management to make necessary changes. This individual would typically also be charged with access to information duties. More specifically with respect to privacy matters, the privacy officer would be responsible for the following:

- Be aware of and current with all privacy best practices.
- Ensure employees of the organization are trained for compliance with applicable privacy legislation. The privacy officer should be the individual with whom employees know to contact with privacy questions and report breaches.
- Ensure that personal information and personal health information in the possession or control of the organization is protected with adequate administrative, technical and physical safeguards. This would include monitoring effectiveness safeguards by tracking all breaches to ensure that safeguards remain effective.
- Respond to privacy breaches in a consistent and timely manner. This would include a thorough investigation of breaches. Investigations should always

include an analysis of applicable privacy laws and internal policies, procedures and other safeguards.
- Respond to privacy complaints in a consistent manner using best practises.
- Liaise with oversight bodies on privacy investigations.

[151] In the course of our investigation of Incident #2, we noted in our letter of August 4, 2010 that:

> Our concern with the above actions of the WCB is that it would appear that the Privacy Officer for the WCB was not involved in this process. We have no comment on the alleged number of phone calls to the Complainant, other than to suggest that if the WCB did place that many calls it demonstrates that it was taking the situation seriously and making concerted efforts to retrieve the breached material. Similarly, we suggest that the content of the letter is appropriate. Again our concern with these actions stems not from the actions themselves, but by whom the actions are undertaken. It would seem most appropriate for the Privacy Officer for the WCB to undertake the actions noted above. It would seem less appropriate when such actions are undertaken by an individual who may have some leadership responsibility for the area of WCB which may have responsibility for the breach having occurred in the first place.

[152] In response, WCB stated in a letter of August 31, 2010:

> I can further advise that the suggestion that the WCB Privacy Officer be involved earlier in the information complaints process would be inconsistent with the manner in which all matters that arise under the workers' compensation system are currently handled. Clients who have concerns with any process are encouraged to speak to their Case Manager as that is the essence of the dispute resolution process within the context of the workers' compensation scheme. It is also to be noted that those who have privacy complaints can appeal in the same fashion that they might appeal any workers' compensation issue, **but in the case of a breach of privacy such an appeal would be handled by the Privacy Officer.**
>
> As has been discussed in the past with your office, given the large volume of mail that is handled by the WCB on a daily basis, it would be impractical that every instance of misdirected mail be referred to the Privacy Officer for investigation. If however there is a complaint regarding a breach of privacy relating to a misdirected letter and the person voicing the complaint is not satisfied with the response received from the Case Manager, those matters are elevated to the level of the Privacy Officer for investigation and recommendations.
>
> [emphasis added]

[153] We again noted our concerns in a letter to WCB dated March 24, 2011:

> We are not suggesting that the core complaint process be changed, we are suggesting however, the Privacy Officer become involved in any process, complaint or otherwise, that involves a privacy complaint, a breach or potential breach of personal information or personal health information in the possession or control of WCB.

[154] WCB responded on May 17, 2011:

> Regarding issue 2 we have noted your concerns but believe nothing would be gained from having all privacy related matters referred to the WCB Privacy Officer. We believe that as soon as, in the judgment of our staff, a significant part of an issue in dispute involves a privacy matter the WCB Privacy Officer would be immediately notified and involved. The staff are aware of the need to notify the WCB Privacy Officer and routinely do so when there are significant issues related to privacy.
>
> How soon the WCB Privacy Officer is contacted is left to the judgment of our staff. Staff are provided guidance in matters of privacy through the WCB Privacy of Information policy and related procedure documents. If they are found not to have followed these policies and procedures this is a matter of discipline that would be addressed by their manager.

[155] The WCB's Policy and Procedure Manual (*Access to Information*) states the following:

> **Information Complaints**
>
> 33. Any person may challenge WCB compliance with its privacy policies and procedures or about its information practices; including accuracy of information collected, recorded, stored or disclosed, or the applicability in particular cases of FOIPP or HIPA. Any such complaints will be addressed by the Corporate Solicitor.
>
> 34. The Office of the Information and Privacy Commissioner (OIPC) may receive complaints under FOIPP or HIPA. Any information received from the OIPC office about such complaints should be immediately sent to the Corporate Solicitor.[28]

[156] The WCB's Policy and Procedure Manual (*Information Complaints* (PRO 07/2008)) states the following:

[28]WCB *Policy and Procedure Manual*: *10.1, Access to Information (POL 06/2008)* at p. 6, available at www.wcbsask.com/WCBPortalWeb/ShowProperty?nodePath=/WCBRepository/pdfs/PolicyManual.

PROCEDURE

1. Persons with complaints should be encouraged to first contact the WCB staff member most closely involved with the circumstances. Responses at this level may be oral or written.

2. If a complaint or concern is received, WCB staff will:

a. Respond to the best of their ability, and record on the claim file or employer account, the steps taken to rectify the complaint, including an apology where needed; or,

b. Refer issues they cannot resolve to their supervisor.

3. When complaints are not resolved by a supervisor, the person will be advised to send a written complaint to the Corporate Solicitor or by e-mail to privacyoffice@wcbsask.com.[29]

[157] In the course of investigating these four incidents we have seen ample evidence to demonstrate that WCB's privacy regime has many shortcomings.

[158] Most notably, the privacy breach report of October 18, 2011 for Incident #4 stated:

> Mid-June, 2011
> A representative from [the health region] contacts the WCB to inquire about the May 2011 ECS as they had not received it. Another ECS is mailed to [the health region].
> ...
> It is also to be noted that [the health region] contacted the WCB in June asking about the May ECS and there is no record of this conversation. In addition, no further action was taken to follow up on the call to determine what may have happened with the original ECS. Finally, the Privacy Officer was not notified in June of this possible breach.

[159] This begs several questions:

- If there is no record of the conversation, how does the Privacy Officer know it existed?
- Were the employees who were notified that the health region did not receive the ECS and did not act upon it disciplined as described above? What was the discipline?

[29] WCB *Policy and Procedure Manual*: *10.5, Information Complaints (PRO 07/2008)* at p. 15, available at www.wcbsask.com/WCBPortalWeb/ShowProperty?nodePath=/WCBRepository/pdfs/PolicyManual.

- Are there other policies that would have instructed this employee to contact WCB's Privacy Officer in this situation?

[160] These questions were asked of WCB via our analysis of May 16, 2012. In response, WCB stated in its letter of July 6, 2012 that:

> Privacy breach protocol was reviewed with all staff after this incident and the importance of documenting and reporting to **their manager** re-emphasised. [emphasis added]

[161] It does not appear that WCB's policies and procedures have a mechanism for employee privacy concerns to be brought internally to the Privacy Officer's attention. Plus, in this case, when the health region brought forward the complaint in Incident #4 to WCB it does not appear to have been resolved or taken to the Privacy Officer, who could have offered advice and taken action to find a solution.

[162] I also believe it is important for an organization's privacy officer to be aware of each breach or potential breach of privacy so that he/she may track and monitor trends or systemic privacy problems. I have commented on the importance of tracking privacy in my Investigation Report H-2007-001.[30]

[163] It is evident from this investigation of these four incidents that there are significant problems with the way WCB processes and handles mail. When looking at the incidents one by one it is easy to chalk each one up to simple human error. Root cause analyses were not performed. However, once incidents are examined together, it becomes evident that the issues involved are systemic and require prompt attention. Further, a root cause analysis is the product of one individual knowing about each incident and tracking them in a meaningful way specifically noting the frequency and severity.

[164] In addition, as noted by WCB's privacy breach report of October 18, 2011, there appears to have been two other potential breaches of privacy identical to Incident #4. These incidents appeared to have occurred in May 2008 and December 2007.

[30]SK OIPC Investigation Report H-2007-001 at [70] to [89], available at www.oipc.sk.ca/reviews.htm.

[165] WCB sent my office copies of its investigation reports of these two incidents occurring in 2007 and 2008. Although it is my office's policy not to launch investigations of breaches that occur more than two years prior, review of these two investigation reports reinforces my concerns. Both of these reports concluded that the breaches occurred as a result of human error, even though an effective procedure of mailing ECSs was not in place. Further, it was recommended that notification not be sent to the affected individuals in these incidents, whereas WCB decided to do so in Incident #4. The reasons for the difference in treatment are not evident.

[166] Finally, with respect to Incident #4, WCB sent notification letters to the 296 claimants whose privacy was breached when the ECSs in question were sent to Business #2. I have obtained copies of three of these letters. They are signed by WCB's Director Case Management South and not the Privacy Officer. Our recommendation to public bodies when giving such notifications of privacy breaches can be found in our resource *Helpful Tips: Privacy Breach Guidelines*. It states:

> **What:** Notifications should include the following information:
>
> - Recognize the impacts of the breach on affected individuals and consider offering an apology;
> - Date of the breach;
> - Description of the breach (a general description of what happened);
> - Description of the breached PI/PHI (e.g. name, credit card numbers, SINS, medical records, financial information, etc.);
> - The steps taken to mitigate the harm to date;
> - Next steps planned and any long term plans to prevent future breaches;
> - Steps the individual can take to further mitigate the risk of harm. Provide information about how individuals can protect themselves e.g. how to contact credit reporting agencies (to set up a credit watch), how to change a health services number or driver's license number;
> - Contact information of an individual within the Organization who can answer questions and provide further information; and
> - That individuals have a right to complain to the OIPC. Provide contact information.[31]

[31]SK OIPC *Helpful Tips: Privacy Breach Guidelines*, at pp. 10 and 11, available at www.oipc.sk.ca/resources.htm.

[167] The notification letter states that "[The ECS] does not include any personal identification numbers or addresses." However, it appears that the ECSs contain work injury claim numbers that would appear to be a personal identification number. The letter asks the recipient to contact the Director Case Management South with any further questions when it is clearly the Privacy Officer who investigated the breach and is recommending actions. Would it not be more useful for an aggrieved individual to speak with the Privacy Officer?

[168] Further, the letter does not include a statement to inform claimants that individuals have a right to complain to my office and does not provide our contact information. It is unclear if such a statement has been included in a notification to Individuals #1, #2, #3 or #4.

[169] A privacy officer would have been familiar with the resources on our website and these best practises. As such, the privacy officer would have been a better choice for the author of the notification letters.

[170] WCB's privacy regime would be better supported if its Privacy Officer had a more active role in each and every privacy breach or potential privacy breach and not just when complaints are received or escalated as suggested by the policy.

[171] Further, it appears that WCB's internal investigation reports lack detail and thoroughness. The lack of tracking and monitoring may lead WCB to superficial treatment that does not allow the discovery of the root cause of a breach. My office's *Helpful Tips: Privacy Breach Guidelines* outlines the following as important elements for internal investigation reports. Emphasized portions indicate what WCB's reports consistently lack.

> The findings of an internal investigation should be recorded in an Investigation Report. An Investigation Report should include the following:
>
> - A summary of the incident and immediate response to contain the breach and reduce harm.
> - Steps taken to contain the breach.
> - Background of the incident.

- Include timelines and a chronology of events.
- **PI/PHI involved (data elements and sensitivity of, number affected, etc).**

- **A description of the investigative process.**
  - **Include the cause of the incident (root and contributing).**
- **A summary of interviews held (complainant, internal, external).**
- **A review of safeguards and protocols.**
- A summary of possible solutions and recommendations.
- **A description of necessary remedial actions, including short and long term strategies to correct the situation (staff training, rework policies/procedures, etc).**
- **A detailed description of what the next steps will be.**
- **Responsibility for implementation and monitoring, including timelines.**
  - **May also include the names and positions of individuals responsible for the implementation.**[32]

[emphasis added]

[172] WCB has not demonstrated that it has an effective and consistent way to monitor, track and respond to privacy breaches in a way that models best practices.

[173] In response to my office's recommendations that WCB change these procedures, its letter of September 11, 2012 stated: "Summary reports are going to be provided quarterly to senior WCB managers, to inform them on the trends… These same managers have been and will continue to receive each investigation report." This action would be welcome.

[174] WCB should allot more resources to the activities of tracking and responding to privacy breaches in order to strengthen its overall privacy regime.

7. What are privacy best practices when retrieving errant personal information?

[175] For Incidents #2, #3 and #4, WCB followed best practices and made attempts to retrieve personal information that had gone astray. However, it seems as though in all cases, the individuals who received the personal information preferred to send the personal

[32] *Ibid.* at p. 7.

information to other authorities and not back to WCB. Complainants B and C brought the personal information to our office. Business #2 brought the personal information to the RCMP who then turned it over to us.

[176] On February 3, 2010, we received a letter from Complainant B dated January 18, 2010 indicating that WCB insisted that he return the personal information mistakenly sent to him. He provided a letter from WCB dated December 11, 2009 addressed to him. The letter threatened fees. It stated:

> This unauthorized retention of materials which are not your property will result in the Workers' Compensation Board taking all legal measures at its disposal to recover these unlawfully retained documents.
>
> I must further warn you that any costs incurred in the recovery of these documents will be recovered from you. Should the Board find it necessary to bring an application to the court to recover the file documents that are unlawfully in your possession, the Board will seek costs against you on a solicitor-client basis. Such costs will in all likelihood be in excess of $1,000.
> In addition, should the party to whom the documents belong commence an action against the Board for the loss of such documents rest assured that you will also be named as a party to any such action.

[177] Best practices suggest that a public body should even go farther in retrieving personal information. An Incident Summary from the Office of the Privacy Commissioner of Canada commended a private business for vowing to send a courier to retrieve any future unauthorized disclosures of personal information as follows:

> When the recipients of the facsimile contacted Viewpoint regarding the transmission they were told to destroy the documentation. Viewpoint indicated to our Office that in future, should any facsimile transmissions containing personal information be sent to the wrong number, Viewpoint will dispatch a courier to retrieve any such records. The company has also taken steps to have all facsimile numbers verified before transmission and has implemented measures to have any incidents reported to management.[33]

[33]Privacy Commissioner of Canada *Summary Incident Summary #1: Misdirected faxes containing health information end up in apartment managers' hands*, available at www.priv.gc.ca/cf-dc/incidents/2004/041221_e.asp.

[178] Further, Nova Scotia IPC Report P-11-01 found that, in a similar mailing incident involving that province's WCB, the public body should incur all expenses for the retrieval of personal information.

> 15) I recommend that the WCB ensure that it recovers *all* personal information it has inadvertently disclosed and it should not be attempting to pass on any costs of doing so. It is not sufficient to rely on the incorrect recipient injured worker or health care provider to destroy the information received. I further recommend that the WCB bear all costs associated with having the personal information returned to or retrieved by its offices.[34]

[179] One further step WCB could take in efforts to retrieve future personal information is to provide the contact information for our office as an alternative for returning the personal information to WCB. As noted, Complainants B and C and Business #2 felt more comfortable with this option. This option is only available however if the individual is aware of the existence of this office.

[180] Further, in Incident #2 and #4, WCB asked Complainant B and the owner of Business #2 to sign affidavits stating that they had not retained any personal information. I applaud this effort.

[181] A letter from WCB dated September 11, 2012 indicates that it intends to provide staff with "more detailed instructions on this point." It is unclear which best practices on retrieving personal information it intends to adopt.

IV FINDINGS

[182] I find both *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act* are engaged in these four incidents.

[34] *Supra* note 16 at p. 38.

[183] I find that, at the time of the incidents, Saskatchewan Workers' Compensation Board had different levels of protection for personal information and personal health information with varying levels of sensitivity but the criteria for such classification was unclear.

[184] I find that even though Complainant A's personal information and personal health information did not end up in the possession of a third party, a breach still resulted.

[185] I find that Saskatchewan Workers' Compensation Board has taken inadequate steps to help prevent breaches similar to Incident #1.

[186] I find the collection of personal information of Individuals #1, #2 and #3 was unsolicited and Saskatchewan Workers' Compensation Board had no authority to collect.

[187] As it appears that all mail received by Saskatchewan Workers' Compensation Board is opened and redirected in the mail room, I find that there is not a mechanism in place to intercept personal information and personal health information in which Saskatchewan Workers' Compensation Board does not have authority to collect.

[188] I find that the centralized services provided by the Saskatchewan Workers' Compensation Board mail room with respect to printing documents, receiving mail and mailing documents was a contributing factor in all of these privacy breaches.

[189] I find Incidents #2, #3 and #4 resulted in unauthorized disclosures of personal information and personal health information.

[190] I find the *Release of Information – Claim Files* procedure was not detailed enough to ensure that claims files would be reviewed before mailing. This is a factor in the unauthorized disclosure of personal information and personal health information in Incident #2.

[191] I find the flow chart mirroring the *Release of Information – Claim Files* procedure is not effective.

[192] In terms of Incident #3, I find that it does not appear that the *Release of Information – Claim Files* procedure was followed. Further, there are other discrepancies in this procedure that prevents it from being effective.

[193] I find that lack of procedures for mailing Employer Cost Statements at the time of Incident #4 was the cause of the unauthorized disclosure of personal information and personal health information.

[194] I find Saskatchewan Workers' Compensation Board's Privacy Officer is not involved in all privacy matters that warrant his attention. Additionally, there does not appear to be a mechanism within the organization to track breaches and monitor compliance.

[195] I find that Saskatchewan Workers' Compensation Board's investigations into these privacy breaches were not sufficiently thorough and its responses lacked consistency and did not follow best practices.

[196] I find Saskatchewan Workers' Compensation Board did not make adequate efforts to retrieve errant personal information and personal health information after unauthorized disclosure to third parties.

V RECOMMENDATIONS

[197] As I previously recommended in Investigation Report F-2007-001[35], Saskatchewan Workers' Compensation Board should revise all policies and procedures to reflect language used in *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act*.

[198] Saskatchewan Workers' Compensation Board should adopt the mailing recommendations I made in Investigation Report F-2007-001 for the mailing of any personal information and personal health information.

[35] *Supra* note 15 at [243].

[199] Saskatchewan Workers' Compensation Board should establish a mechanism to return or destroy unsolicited personal information and personal health information at the point of collection.

[200] Saskatchewan Workers' Compensation Board employees should be educated on unauthorized collections of personal information and personal health information and what to do in the event of an unsolicited collection.

[201] All mailing procedure documents should be amalgamated into one document that reflects best practices on mailing all personal information and personal health information.

[202] The term "claim owner" should be defined in the *Release of Information – Claim Files* procedure document. Policies and procedures should use specific position titles and not slang or proper names for the sake of clarity and keeping material up-to-date.

[203] Mailing procedures should include specifics on why documents need to be reviewed, who should review them and what should be looked for during the review.

[204] Saskatchewan Workers' Compensation Board should improve the manner in which it tracks, reports and monitors privacy breaches in order to better identify systemic issues.

[205] Saskatchewan Workers' Compensation Board should improve the ways it investigates and responds to privacy breaches, including more detailed investigation reports and consistent responses that reflect best practices.

[206] Saskatchewan Workers' Compensation Board should ensure that the privacy officer has sufficient resources to fulfill the roles outlined at paragraphs [150] and [153].

[207] Saskatchewan Workers' Compensation Board should follow best practices when attempting to retrieve personal information and personal health information after

unauthorized disclosure such as offering to send a courier to pick up the information and suggesting, as an alternative, that it can be entrusted to my office.

Dated at Regina, in the Province of Saskatchewan, this 25th day of October, 2012.

R. GARY DICKSON, Q.C.
Saskatchewan Information and Privacy Commissioner