



Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. PC-010054-1

Workplace Safety and Insurance Board



80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

80, rue Bloor ouest
Bureau 1700
Toronto (Ontario)
M5S 2V1

416-326-3333
1-800-387-0073
Fax/Télééc: 416-325-9195
TTY: 416-325-7539
<http://www.ipc.on.ca>

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. **PC-010054-1**

MEDIATOR: **Shaun Sanderson**

INSTITUTION: **Workplace Safety and Insurance Board**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

The Workplace Safety and Insurance Board (the WSIB) notified the Office of the Information and Privacy Commissioner/Ontario (the IPC) about a breach of the *Freedom of Information and Protection of Privacy Act* (the *Act*). The WSIB advised the IPC that a client (client #1) who had requested access to his own WSIB claim file had also received documentation from another individual's claim file (client #2). As a result, a privacy investigation was initiated by the IPC.

In a follow-up letter to this office dated November 15, 2001, the WSIB's FOI Coordinator explained that, in May 2001, the WSIB had sent client #1 a copy of his own claim file, but had inadvertently attached a copy of an unrelated file belonging to client #2. Upon notifying an adjudicator of this incident, client #1 was advised that the documents were confidential and must be returned to the WSIB immediately, and that a WSIB investigator would be sent to retrieve the entire package. Client #1 advised that he would prefer to return the package to the WSIB's office on the following day, and subsequently met with the access manager who reviewed the entire file and removed all documentation relating to client #2.

Approximately six months later, client #1 advised the adjudicator that he had kept a copy of the documents relating to client #2. At this time, the adjudicator contacted the FOI Coordinator who then initiated an internal investigation and notified the IPC.

ISSUES ARISING FROM THE INVESTIGATION:

The following issues were identified as arising from the investigation:

(A) Was the information in question "personal information" as defined in section 2(1) of the *Act*?
If yes,

(B) Was the disclosure of the personal information in accordance with section 42 of the *Act*?

RESULTS OF THE INVESTIGATION:

Issue A: Was the information in question “personal information” as defined in section 2(1) of the Act?

Section 2(1) of the Act states, in part:

"personal information" means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

...

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

The information in question was a copy of client #2's WSIB claim file which included forms, memos and correspondence containing details of his workplace accident, his medical information, age, address, telephone number, financial compensation and other information about him. In my view, the records in question contain personal information as contemplated by section 2(1) of the *Act*. The WSIB does not dispute this finding.

Conclusion: The information in question was personal information as defined in section 2(1) of the *Act*.

Issue B: Was the disclosure of the personal information in accordance with section 42 of the Act?

Section 42 of the Act sets out the rules for disclosure of personal information other than to the individual to whom the information relates. This section provides that an institution shall not disclose personal information in its custody or under its control, except in the circumstances listed in sections 42(a) through (n). Having reviewed these provisions, I find that none of these circumstances were present in this case. The WSIB acknowledges that the disclosure of client #2's claim file to client #1 was not in accordance with section 42 of the *Act* and there is no

dispute that this incident should not have occurred. WSIB states that it sincerely regrets this unfortunate incident.

Conclusion: The disclosure of the personal information was not in compliance with section 42 of the *Act*.

OTHER MATTERS:

Requesting a copy of a WSIB claim file

An injured worker may receive access to his or her own WSIB claim file by making a request to the Access Branch. Representatives and other parties can only receive access to a claim file with the written authorization of the injured worker. A request for access to a claim file is processed by the Access Branch in accordance with the guidelines set out in the *Access Branch Information Guide*, which was revised in August 2001. A copy of this guide has been provided to the IPC for review. The procedures for processing access requests are as follows:

- Access Telephone Clerks receive requests for claim files via letter, memo or telephone. They input the information on the Access Tracking System, which notifies the Records Control Department to begin searching and printing copies of the posted files.
- When the copies are printed and delivered to the Access Department, an Access Support Clerk receives them and assigns them to an Access Review Clerk for processing.
- Upon receiving the assigned file, the Access Review Clerk examines the file to ensure that the correct information is being sent to the appropriate party with the proper covering letters and forms. Once the files are assessed, the Access Review Clerk packages and addresses them for mailing.

It should also be noted that, as a routine practice, a Notice is sent out with every file, advising recipients to contact the WSIB if they find any documents that do not belong to the claim file. The Notice also states that the information is confidential and should not be released to anyone else. A copy of this Notice has been provided to the IPC for review. In my view, this proactive measure is a good practice, as it helps to ensure that if a privacy breach does occur, that it is dealt with in a proper manner.

How did client #2's claim file end up being mailed to client #1?

Upon completion of its internal investigation, the WSIB advised that, while it is not possible to determine the exact cause of this mistake, it appears that the error occurred because the WSIB employee who mailed the package to client #1 did not verify the separation of the files during the mailing process, as required. In a letter to the IPC dated March 20, 2001, the FOI Coordinator explained that the error involved the sending out of a file from a regional office that included a file from another regional office. Because electronic files are printed at the WSIB's Head Office

in Toronto and returned to the regional office for mailing, she concluded that it is logical to assume that the error occurred during the printing process, rather than the mailing/access process.

The FOI Coordinator further explained that the Records Control Department has a system restriction of inputting print requests for claim files exceeding ninety-nine pages. Any claim exceeding this amount requires user groups to break down each claim into several parts before inputting. Once the print is received, this requires extended time and effort in sorting the various parts of a claim file into one package before being forwarded to the Access Department. The FOI Coordinator acknowledged that this system restriction greatly increases the likelihood of sorting errors occurring at the Records Control Department. However, she notes that the access review clerk should have caught the mistake during the access review and mailing process.

Steps taken by the WSIB in response to the disclosure

Upon learning of this incident, the WSIB's FOI Coordinator immediately initiated an internal investigation and notified this Office about a breach of the *Act*. The WSIB then took the following steps in response to the disclosure:

- As noted above, this incident was initially reported to an adjudicator in May 2001 and steps were taken by the WSIB to retrieve the records at issue. However, the adjudicator was later advised that client #1 had kept his own copy of the documents belonging to client #2. When advised of this situation, the FOI Coordinator immediately contacted client #1 to discuss the seriousness of this matter and to advise him that the IPC had been notified. She also sent him a follow-up letter dated November 27, 2001. He subsequently agreed to return all outstanding copies of the records to the WSIB. On November 29, 2001, client #1 returned the records to the WSIB and signed an undertaking, confirming that he has not retained any copies of the claim documents pertaining to client #2.
- The FOI Coordinator also sent a letter to client #2, dated November 15, 2001, to advise him about the breach of his personal privacy and to offer an apology for this regrettable error.
- On November 6, 2001, the Manager of the Access Department met with all access staff to remind them to thoroughly examine each file prior to sending it out to ensure that it does not contain documents relating to another individual. Staff were also reminded about the mailing procedures and sorting guidelines contained in the *Access Branch Information Guide*.
- It is highly likely that the problem first occurred in the Records Control Department as a result of the system restriction discussed earlier. To help prevent such sorting errors from re-occurring in the future, the WSIB has implemented changes to the system. The FOI Coordinator advised the IPC that a "host print enhancement" was implemented on March 4, 2002. This was designed to eliminate the system restriction of inputting print requests

for claim files exceeding ninety-nine pages. With the enhancement, it is no longer necessary to break down the files into various inputs and sort the outputs into one file. All files are now being received as one complete package.

CONCLUSION:

I commend the WSIB's FOI Coordinator for her actions upon learning of this incident, and for implementing a permanent measure which will significantly reduce the chances of a similar situation from occurring in the future. As well, WSIB officials should be commended for the steps they have taken to address this particular situation on a systemic basis, through the "host print enhancement" and elimination of the system restriction.

I have reached the following conclusions based on the results of this investigation:

1. The information in question was personal information as defined in section 2(1) of the *Act*.
2. The disclosure of the personal information was not in compliance with section 42 of the *Act*.
3. The disclosure was inadvertent, through human error. The WSIB has taken appropriate measures to ensure the protection of personal information in the future and to prevent a similar incident from reoccurring.

Learning of a Privacy Breach

Once an institution learns that a possible privacy breach has occurred, immediate actions should be taken. In a publication entitled "*A Privacy Breach Has Occurred – What Happens Next?*" the IPC has suggested the following actions to assist in controlling a privacy breach:

- Identify the scope of the breach and take steps to contain the damage (for example, this may involve retrieving hard copies of personal information that have been disclosed, determining whether the privacy breach would allow unauthorized access to an electronic information system, changing file identification numbers);
- Ensure that appropriate institution staff is immediately notified of the breach, including the FOI Coordinator, the head and/or delegate;
- Immediately inform the IPC of the breach;
- Notify individuals whose personal information has been disclosed;
- Conduct an internal investigation into the matter, report on the findings and quickly implement any recommendations. The objectives of this investigation should include a

review of the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal information;

- Address the situation on a systemic basis. In some cases, program-wide or institution-wide procedures may warrant review, such as in the case of a misguided fax transmission. Ensure that policies, procedures and staff training are adequate across the board; and
- Try to resolve a complainant's concerns informally, at the onset of the complaint.

Because the FOI Coordinator was not immediately notified about this particular breach, some of these steps were initially overlooked, one of which was notifying the individual whose personal information was at issue. Given her expertise, the FOI Coordinator is in the best position to ensure that appropriate actions are taken with respect to breaches of personal privacy. Accordingly, I am making the following recommendation:

RECOMMENDATION:

I recommend that the WSIB notify all staff that, in the rare instances where there are breaches of the *Act*, that the FOI Coordinator should be immediately notified so she can ensure that all steps are taken to properly address the matter.

The WSIB should provide the Office of the Information and Privacy Commission/Ontario with proof of compliance with the above recommendation by December 9, 2002.

Shaun Sanderson
Mediator

September 9, 2002