Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PC-010045-1

Ministry of Community and Social Services

March 6, 2002

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/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. **PC-010045-1**

MEDIATOR: **Giselle Basanta**

INSTITUTION: **Ministry of Community and Social Services**

SUMMARY OF COMPLAINT

The Information and Privacy Commissioner/Ontario (the IPC) received notification verbally, and subsequently in writing from the Ministry of Community and Social Services (the Ministry), that the Ministry received an access request pursuant to the *Freedom of Information and Protection of Privacy Act (*the *Act)*, but was unable to locate the corresponding file in order to respond to the request. The Ministry explained that in the process of transferring the corporate client file of an individual receiving assistance through the Ontario Disability Support Program (ODSP) from one office (the sending office) to another office (the receiving office), the file had gone missing. As a result, a privacy complaint was initiated by the IPC.

DISCUSSION

The following issues were identified as arising from the investigation:

Is the information contained in the missing file "personal information" as defined in section 2(1) of the *Act*?

Section 2(1) of the *Act* provides, 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,
>
> (e) the personal opinions or views of the individual except where they relate to another individual,
>
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
>
> (g) the views or opinions of another individual about the individual, and
>
> (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 Contents of the File

The Ministry advised that the file pertains to a client of the ODSP and would typically contain personal information such as an client's name, address, telephone number, medical, financial, employment and family information and the personal information of any dependents. This personal information, including birth verification, health insurance card number and Social Insurance Number, would have been necessary to determine eligibility for certain programs and required for the completion of mandatory application forms and any related documentation and/or correspondence.

Although the specific contents of the file are unknown, in this case, the Ministry took the position that it was unlikely that the file would contain the personal information of anyone other than the client and any dependents.

I conclude that the information is clearly personal information as contemplated in section 2(1) of the *Act*. The Ministry does not dispute this.

In the absence of evidence that the Ministry disclosed any information contrary to section 42 of the *Act*, I will consider whether appropriate file transfer procedures were in place "to prevent unauthorized access to the records" and whether such "reasonable measures" were "defined, documented and put in place, taking into account the nature of the records to be protected" pursuant to section 4(1) of O. Reg. 460.

Did the Ministry define, document and put into place reasonable measures to prevent unauthorized access to the record in accordance with section 4(1) of O. Reg. 460?

Section 4(1) of O. Reg. 460 provides:

> **4.** (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

Steps taken by the Ministry as soon as it was known the file was missing

Notification by the Ministry

The Ministry confirmed that the client to whom the information in the missing file relates, was contacted and advised accordingly. The client was assured that the Ministry was conducting a thorough search for the file and that the client would be kept informed as to the ongoing status of the search. The Ministry offered an apology to the client.

Ministry action at the receiving office

The Ministry explained that the client had moved and as a result, the file was transferred by courier, from one office to another. The Ministry confirmed with the courier company that the file was delivered, but at the receiving office a signature was not required so it was not possible to determine who actually received the file. The Ministry advised that this practice has since been changed and a signature is now required upon receipt of transferred files. At the receiving office, a thorough search of all file rooms was conducted. Specifically, the search consisted of:

- Thorough search of the receiving office's file rooms
- Request to all staff on two occasions to conduct a thorough search for the file at their workstations
- Request to other local offices in the region to check their file rooms and staff workstations
- Contact with the sending office to confirm that the file was sent
- Confirmation that a file room sign out card was created for the file

Ministry action at the sending office

- Thorough search of the sending office's file rooms
- Review of the sending office's records relating to the transfer of the file
- Provision to the receiving office of the courier documents indicating the date of service, the manual record in their Transfer Log Book indicating that the physical file was sent to

the receiving office, and confirmation that the file tracking system indicated a "delivered" status to the receiving office

Results of the Search

The Ministry determined that an electronic file transfer transaction record was completed on its file tracking system. However, with respect to the transfer of the physical file, the manual logbook at the receiving office was not updated to reflect the date that in the physical file was received and who received it.

Remedial Steps taken by the Ministry

In a letter to Assistant Commissioner Tom Mitchinson, the Freedom of Information Co-ordinator at the Ministry advised this office that the file tracking system at the receiving office was immediately reviewed and enhanced as a result of this incident. The Co-ordinator indicated that an interim process was put into place in October 2001 and would be reviewed again in November 2001 when a new computer system, SDMT is put into place. It was agreed that the Ministry would provide the Mediator with an update once the audit was completed.

According to the report from the Ministry, as a result of this incident, the Ministry took three specific actions:

- A physical search of the sending and receiving offices and any other local offices in both those regions
- The implementation of new business procedure for file handling and,
- A file audit of the receiving office and other local offices in that region

The Physical Search

The aspects of the physical search conducted by the Ministry have already been outlined.

Implementation of New Business Procedures for File Handling

The File Tracking Procedures at the receiving office were reviewed and enhanced in October 2001 and again in November 2001 as a result of the implementation of new service delivery technology (SDMT).

The updated process used at the receiving office when a physical corporate file is transferred from another ODSP office is as follows:

1. Client files are normally sent from one office to another via a courier service

2. The staff person at reception will accept courier deliveries.

3. Income Support Clerks (ISC) on mail duties open the courier packages and arrange for proper distribution.

4. A manual logbook (the "Transfer-In Logbook") is used for recording the receipt of all client files received via courier.

5. The ISC updates this logbook regularly as courier packages are opened and sorted for distribution.

6. The following details are recorded in the logbook:

   a) Date received
   b) Courier log number or bar code from package
   c) Originating office
   d) Detailed listing of corporate files
   e) Distribution of the file

7. The files are placed in the designated holding spot in the internal mail slots pending being keyed into SDMT by the ISC.

8. The ISC pulls files daily from this holding spot in order to complete the electronic file transfer on the SDMT system by changing the office name on the File Transfer Screen to reflect that the file is now physically located in the office. The ISC appends the "Note" in SDMT to reflect that the file was received and assigns the file to the appropriate office.

9. After the electronic process is completed, a sign out card is completed for the file for use in the file room and the files are distribute to the appropriate staff for action.

10. Any paperwork received from the client while the file is in transit is kept in a manila folder to be filed once the physical file is received.

11. The Terminal Room ISC has two additional cross checks to ensure that that the physical corporate file is received for all electronic transfers:

    i) On a daily basis, the ISC prints the 'Unassigned File Transfers' list from SDMT. This list is used to monitor when the physical file actually arrives and the received date is also noted on this list. Files still not received after 7-10 working days, the ISC will contact the sending office to follow-up on when the physical file will be couriered.

    ii) Also, once a week, the Terminal Room ISC will review the contents of the manila folder and determine if follow-up on any files not yet received is required.

The File Audit

A file room audit was completed in all the ODSP offices in the same region as the receiving office to confirm the physical presence of all files.

CONCLUSIONS

I commend Ministry staff for their actions after learning that the client's ODSP file containing that individual's personal information had gone missing and for the steps taken by the Ministry to conduct a thorough search in multiple locations for the missing file.

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

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

2. The Ministry conducted a thorough search, but was unable to locate the file containing personal information relating to a client and possibly any of that client's dependents receiving assistance under the ODSP.

3. I am satisfied with the notification provided to the client by the Ministry in the circumstances.

4. The measures that were previously in place by the Ministry to prevent unauthorized access to the record were not in accordance with section 4(1) of O. Reg. 460.

5. The Ministry acknowledges that the result of its search confirmed that at the receiving office, a signature was not required upon delivery of the file by the courier company, therefore the manual logbook was not updated to reflect the date that the physical file was received and who actually received the file.

6. However, the Ministry has now put into place updated corporate file tracking procedures that form part of a new computer system, SDMT for file handling in order to remedy this situation. As a result, the Ministry has taken significant steps to meet its obligations under section 4(1) of the O. Reg. 460.

RECOMMENDATIONS

In addition to the remedies already put into place by the Ministry, I recommend the following:

1. The Ministry should use a bonded courier service for the purpose of transferring physical corporate client files from one office to another. (See paragraph 1 of the Corporate File Tracking Procedures dated November 30, 2001)

2. The Transfer-In logbook should be used to track and document each person that handles the transferred file at the receiving office at every point in this process. It is important that the Ministry be able to connect the receipt of the physical file to the staff member(s) charged with handling the administrative duties of the transfer of the physical file. (See paragraphs 1-6)

3. The "designated holding spot" should be in a secured location. (See paragraph 7)

4. The manila folder containing any "paperwork received from the client while the file is in transit" should be kept in a secured location. (See paragraph 10)

The Ministry should provide the Office of the Information and Privacy Commissioner with proof of compliance with the above recommendations no later than May 24, 2002.

March 6, 2002

Giselle Basanta
Mediator