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-030013-1

Ministry of Health and Long-Term Care

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-030013-1**

MEDIATOR: **Frances Soloway**

INSTITUTION: **Ministry of Health and Long-Term Care**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

The Office of the Information and Privacy Commissioner (the IPC) received a telephone call from a Director of the Registration and Claims Branch, Ministry of Health and Long Term Care (the Ministry) regarding the theft of 15 Ontario Health and Insurance Plan (OHIP) health cards. Specifically, he indicated that a client at one of the OHIP offices reached over the top of a counter and took 16 returned and voided health cards, which the clerk had left on the computer. As a result, the IPC initiated a privacy complaint under the *Freedom of Information and Privacy Act* (the *Act*).

PARTICULARS OF THE INCIDENT

During the course of our investigation, the Ministry provided this office with a document titled *Summary Of Steps Taken, Ottawa Stolen Cards Case*, copies of certain e-mails, letters, a Business Communication and a copy of relevant sections of the Ministry's Security Policy Manual. Also during the investigation, I had numerous discussions with the senior Manager, Regional Operations. As a result, I obtained the following details regarding the incident in question:

The event occurred at 1630 hours on Wednesday, March 11, 2003 at one of the Ministry's OHIP offices in Ottawa. At this time a clerk left her counter to speak with her manager at an irate client's request. When she returned the client was gone. Around 1700 hours when the clerk was preparing to take all the voided OHIP cards she had collected during the day to the confidential "shred–it-bins", she noticed that the voided cards she had collected that day were missing and notified her manager. The clerk and the manager then checked the confidential "shred-it-bins", however the cards were not there. The manager and the team leader then viewed the closed circuit television (CCTV) tape of the relevant counter. The tape confirmed that the irate client referred to above had reached over the counter and grabbed the returned voided health cards

from the computer on the lower ledge of the counter while the clerk had gone to speak to her manager. The Ottawa City Police were subsequently called by the manager and advised of the situation. The CCTV tape and the details were provided to the constable who attended the premises and viewed the tape. The police later recovered all of the stolen health cards. The police have also laid charges with respect to this incident and the matter is currently before the courts.

Steps taken by the Ministry:

A. At the Ottawa office

- As mentioned above, the Ministry contacted the police who recovered all of the stolen voided health cards**.**

- The manager immediately reviewed the Ministry's security protocols with the clerk and a verbal reprimand was given.

- The security protocols were then reviewed with the 35 customer service staff comprised of 13 regular classified clerks, 12 outreach clerks and 10 ad hoc clerks (on-call).

- A complete audit of all the transactions performed at the counter in question on March 11, 2003 was undertaken in order to reconcile the number of cards. The clerk at this counter had completed a total of 25 transactions. Fifteen of these resulted in returned cards and the sixteenth was the irate client's own card. Fourteen of the holders of the returned now voided cards were contacted by telephone by the Ottawa Service Manager. These persons were advised that their returned voided cards had been stolen and had subsequently been recovered by the police. One client was not reachable by telephone and instead he was sent a letter. The Senior Manager, Regional Operations reports that all 15 clients were grateful for the notice and there have been no further concerns.

- A memo was issued immediately following the incident to all the customer service staff stating that all returned health cards were to be cut in half and all pieces placed in a locked "shred-it-bin" for confidential disposal **immediately** upon receiving a card. Staff were advised that failure to comply would result in disciplinary action.

- The Service Manager arranged for two more bins to be installed so that each Section has easy access to a "shred-it-bin" for returned cards. These additional bins have been in place since March 16, 2003.

- The Team Leader and the Service Manager implemented and currently maintain regular "rounds" throughout the day to ensure compliance with the security policy.

B. Throughout the province

- An Administrative-Security Business Communication (BusCom) was issued to the approximately 424 customer service clerks in the Regulation and Claims Branch throughout the province. This BusCom indicated the importance of cutting up the returned health cards **immediately** upon collection and processing the change on the Registered Persons Database (RPDB).

- All regional management staff were directed to follow up with discussion at unit meetings. Follow up by the Ministry has shown that regional management staff have discussed this security protocol in all 26 OHIP offices at unit meetings with customer service staff.

- The Senior Manager, Regional Operations initiated a request to the Security Manager to review card destruction practices at field offices. This is currently underway.

The Ministry also advised that during its investigation into this matter it discovered a systems shortcoming in the RPDB. Specifically, if a client reports their card lost and the initial reporting has taken place on the system, the system will not allow another change to that record if the client subsequently finds their card at a later date and brings it in to an OHIP office. This means that the system would not be able to produce a "total" amount of cards returned at the end of the day. The Ministry is currently undertaking a review in order to address this.

DISCUSSION:

The following issues were identified as arising from this privacy complaint investigation:

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

Section 2(1) of the *Act* states, in part, that "personal information" means recorded information about an identifiable individual.

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,

(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;"

Of the cards stolen 10 were photo health cards and 6 were the older red and white cards. As the cards were voided, they were no longer valid for health care service purposes. However, they could potentially be used for identity falsification purposes. On the front of a photo health card is the name, date of birth, gender, photograph, signature, date of issue of card and date of expiry. On the back is the address of the card holder, and organ donor information. The older red and white cards contain the name of the holder of the card and health number.

As defined in section 2(1) of the *Act*, I find that the information on both types of health cards clearly contains "personal information". The Ministry does not dispute this finding.

Was the disclosure of the "personal information" in accordance with section 42 of the *Act*?

Section 42 of the *Act* sets out a number of circumstances under which an institution may disclose personal information. Clearly, in situations where there has been a theft of personal information, none of these circumstances apply. The disclosure, therefore, was not in accordance with the *Act*.

Were reasonable measures in place to prevent unauthorized access to the records?

Section 4(1) of Regulation 460, made under the *Act*, states that "[e]very 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".

As indicated above, the Ministry provided this office with relevant sections of its Security Policy Manual, which contains the security policy of the OHIP. Specifically the section on ***Disposal of Obsolete Health Cards*** states:

- Health cards returned by registered persons shall be removed from the RPDB and disposed via the Confidential Plastic Waste Disposal system. It may require temporary secure storage to ensure sufficient quantity is accumulated to make the disposal cost efficient….

  NOTE: All health cards returned must be made non-re-usable after it is removed from the RPDB, i.e., cut in two or more pieces.

Despite this policy, in this case, the clerk did not make the returned cards non-re-usable after she received them and removed them from the RPDB. As it was a busy day, the clerk left the returned voided health cards on the computer on the lower ledge of the counter. At the end of the day she was planning to cut all of the cards she had received that day in half and place them in the "shred-it-bin".

In light of the above, I am satisfied that reasonable measures were in place to prevent unauthorized access to the records, however, these measures were not followed in this case. In order to emphasize the importance of making the returned cards non-re-usable **immediately** upon receiving them and removing them from the RPDP, I will be recommending that the Ministry amend its policy in order to explicitly state this.

CONCLUSION:

I have reached the following conclusions based on the results of my investigations:

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

2. The disclosure was inadvertent as it was caused by the theft of a number of returned and voided OHIP cards.

3. Reasonable measures were in place to prevent unauthorized access to the records, however, these measures were not followed in this case.

RECOMMENDATIONS

Taking into consideration the privacy-protective work already done by the Ministry in relation to our investigation into this matter I recommend the following:

1. I recommend that the Security Policy Manual's section on *Disposal of Obsolete Health Cards* be amended to clearly state that returned voided health cards be cut in two or more pieces and placed in the confidential "shred-it-bins" **immediately** upon receiving them on a one by one basis.

2. I recommend that the card destruction practices review at all field offices currently underway by the Security Manager be completed and recommendations considered and implemented where appropriate. (For example, whether additional locked "shred-it-bins" may be required at other offices.)

3. I recommend that the Ministry complete it's review of the RPDB, as outlined above and initiate a process to make the necessary changes to the system.

By **November 24, 2003** the Ministry should provide the IPC with proof of compliance with the above recommendations.

August 25, 2003

Frances Soloway
Mediator