



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

INVESTIGATION REPORT

INVESTIGATION I93-046P

MINISTRY OF HEALTH



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/Télé: 416-325-9195
TTY: 416-325-7539
<http://www.ipc.on.ca>

INTRODUCTION

Background of the Complaint

This investigation was initiated as a result of a complaint concerning a psychiatric hospital of the Ministry of Health (the Ministry).

A hospital employee was concerned that the hospital was storing employee related injured worker information with regular patient information on a computer system that was accessible by other employees who did not need access to this information. He was also concerned that pay stubs were distributed in an unsecured manner, and that employee time sheet printouts showing employees' Social Insurance Numbers (SINs) were being sent to the departments in an unsecured manner.

The complainant believed that these practices were in contravention of the Freedom of Information and Protection of Privacy Act (the Act).

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?
- (C) Were reasonable measures in place to prevent unauthorized access to "personal information" in accordance with Regulation 460 under the Act, as amended by Regulation 532/93?

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,

- (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,

- ...
- (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;

We have determined that injured worker information was comprised of the injured worker's name, the type of injury, the amount of time away from work and whether a Workers' Compensation Board (WCB) claim had been made. Pay stubs and time sheets contained the employee's name and SIN. Pay stubs also contained salary details.

We are of the view that this information met the requirements in paragraphs (b) and (h) of the definition of personal information in section 2(1) of the Act.

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?

Under the Act, personal information in the custody or under the control of an institution can not be disclosed except in the specific circumstances outlined in section 42.

Pay Cheques/Pay Stubs

The Ministry stated that it had relied on section 42(d) of the Act for the disclosure of personal information contained in the pay cheques/pay stubs. Section 42(d) states:

An institution shall not disclose personal information in its custody or under its control except,

- (d) where disclosure is made to an officer or employee of the institution who needs the record in the performance of his or her duties and where disclosure is necessary and proper in the discharge of the institution's functions;

The complainant was concerned that pay-stubs were not distributed in sealed envelopes.

In our draft report, we stated that under the Ministry's "Payroll Procedures", pay cheques/pay stubs were being distributed to staff through supervisors or delegates. Staff not on duty on pay day could pick up their cheques at the Business Office. The Ministry stated that only 4 out of 750 staff had requested that their pay stubs be placed in a sealed envelope.

While we accept that it was the duty of the supervisors or delegates to distribute pay cheques/pay stubs to employees, it is our view that they needed to know only the names of the employees in

order to perform this duty. The disclosure of any other personal information about employees to supervisors or delegates in the distribution of pay cheques/pay stubs was not in accordance with section 42(d) of the Act.

We also examined the other provisions of section 42 of the Act and determined that none were applicable in the circumstances of this case.

Conclusion: The disclosure of personal information other than the names of employees to supervisors or delegates who distributed employees' pay cheques/pay stubs was not in accordance with section 42 of the Act.

In its submissions to our draft report, the Ministry advised that in October 1993, new payroll procedures were initiated that provides for greater protection of personal information. The new payroll procedures required all staff to pick up their own pay cheque/pay stub personally from the Business Office. It was the Ministry's view that the new procedures eliminated the need to seal pay cheques/pay stubs in envelopes.

Computer Printouts of Time Sheets

The Ministry stated that it was its view that disclosure of employees' SINs on computer printouts to certain staff was in accordance with both sections 42(c) and 42(d) of the Act.

As previously indicated, section 42(d) permits the disclosure of personal information where the disclosure is made to an officer or employee of the institution who needs the record in the performance of his or her duties and where disclosure is necessary and proper in the discharge of the institution's functions.

The Ministry stated that SINs were needed to key date into the computer for payroll entry. The Payroll Department sent computer printouts of time sheets, which included employees' SINs, to Head Nurses, Supervisors, Department Heads and other managers for their input of the number of hours their assigned staff has worked. The completed time sheets were then returned to the Payroll department for processing. The payroll department needed the SINs as the sin was used as a unique employee identifier for entering data into the government payroll system. The Payroll Department had no way of keying in employees' worked time data into the payroll system without this unique identifier. It was the Ministry's view that SINs were not included on the timesheet printouts before they were sent to staff of other departments, the payroll staff would not be able to enter the time worked information into the computer, when the time sheets were returned to them.

It is our view that the administration of employees' pay, specifically data entry of salary information is a function of the Ministry and that the disclosure of employees' SINs was necessary to the payroll staff in order for them to be able to key into the government payroll system. Therefore, the disclosure of the employees' SINs to the Payroll Department staff was in accordance with section 42(d) of the Act. However, it is our view that the disclosure of the SINs to staff of other departments, i.e. Head Nurses, Supervisors, Department Heads and other Managers was not necessary for them to be able to complete employees' time sheets. Therefore,

the disclosure of employees' SINs to the staff in other departments was not in accordance with section 42(d) of the Act.

We also examined the application of section 42(c) of the Act to the disclosure of employees' SINs. This section states:

An institution shall not disclose personal information in its custody or under its control except,

- (c) for the purpose for which it was obtained or compiled or for a consistent purpose;

The employees' SINs were collected as a unique identifier by the Payroll Department staff so that they could enter employees' time worked data into the government payroll system. In our view, the disclosure to staff in other departments of employees' SINs on computer printouts of time sheets sent to them, could not be said to be for this same purpose or for a consistent purpose. The disclosure to them was, therefore, not in accordance with section 42(c) of the Act.

We have examined the other provisions of section 42 and have determined that none were applicable to the disclosure of employees' SINs to staff who were not in the Payroll Department.

Conclusion: The disclosure of employees' SINs on computer printouts of time sheets to staff in the Payroll Department was in accordance with section 42 of the Act.

The disclosure of employees' SINs on computer printouts of time sheets to staff in other departments was not in accordance with section 42 of the Act.

Issue C: Were reasonable measures in place to prevent unauthorized access to "personal information" in accordance with Regulation 460 under the Act, as amended by Regulation 532/93?

Section 4(1) of Regulation 460 under the Act, as amended by Regulation 532/93 states:

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.

Computer Printouts of Time Sheets

The complainant was concerned that the computer printouts of time sheets showing employees' SINs were being sent to departments in an unsecured manner. He stated that time sheets were left open on the responsible individuals' desks and could be read by anyone.

The Ministry stated that computer printouts of time sheets from the Payroll Department were distributed to and returned from other departments in sealed envelopes. The Ministry further stated that according to its procedures, individuals responsible for completing the information on time sheets should not have had time sheets open on their desks in a way which allowed others to read them. However, the Ministry acknowledged that there may have been isolated incidents where there may have been non-compliance with these procedures.

It is our view that there were reasonable measures documented and defined for the protection of personal information contained in computer printouts of time sheets when they were distributed to departments heads; when they were in the possession of department heads; and when they were returned to the Payroll Department. However, individual staff may have not have been following the appropriate security procedures at all times.

Conclusion: Reasonable measures to protect computer printouts of time sheets in the departments were defined, documented and in place, in accordance with section 4(1) of Regulation 460 under the Act, as amended by Regulation 532/93.

Employee related information

The complainant was concerned that the Ministry was storing employee related injured worker information with regular patient information on a computer system that was accessible by other employees, who did not need this information.

The complainant also stated that another employee had sought counselling and assistance from doctors at the hospital and that this employee's personal information had then been stored in the regular patient computer system and was, thus, accessible by other employees who did not need access to employee-related information. The complainant, however, was unable to provide any documentation to support his contention about this incident.

The Ministry stated that the computer used to track employee incidents including WCB claims, was a stand alone personal computer that was located in the office of the Co-ordinator of Occupational Health and Safety, and was distinct from the hospital's computer system that contained regular patient information. This personal computer was not networked with any other computer system in the hospital. Further, the software in use had a password to prevent unauthorized personnel from accessing the information stored on the computer.

The Ministry indicated that only the Co-ordinator of Occupational Health and Safety, who was responsible for workers' compensation claims management, had access to the information on the computer. Any requests for information had to be first approved by the employee and then the administration of the of the hospital before it could be released.

The Ministry stated that it was aware of the incident described by the complainant but that it had subsequently taken certain corrective measures. The new procedures were follows.

Employees who obtained professional help from the hospital were treated as regular patients but, their medical case book and all related documents were kept in locked cabinets under the custody and control of the Director of Clinical Records Services. The computerised medical records of these employees were continued to be kept in the hospital's regular patient computer system. However, in the computerised records, the employee's name was changed to an alias, and other identifying information such as address, next of kin, SIN and Health Card Number was recorded as "unknown". The key to all alias name in the computer was kept in the log in the confidential drawer by the Director of Clinical Records Services.

The Ministry stated that these procedures were documented in the Clinical Records Departmental manual.

Based on the above information, it is our view that reasonable measures were defined, documented and in place to prevent unauthorized access to the personal information of employees with respect to employee incidents including injured worker information. Similarly, measures were in place with respect to personal information, relating to those employees who had obtained professional help, which was stored in the hospital's regular patient computer system.

Conclusion: Reasonable measures were defined, documented and in place to prevent unauthorized access to employee-related personal information stored in the hospital's computer system in accordance with section 4(1) of Regulation 460 under the Act, as amended by Regulation 532/93.

SUMMARY OF CONCLUSIONS

- The information in question was "personal information" as defined in section 2(1) of the Act.
- The disclosure of personal information other than the names of employees to supervisors or delegates who distributed employees' pay cheques/pay stubs was not in accordance with section 42 of the Act.
- The disclosure of employees' SINs on computer printouts of time sheets to staff in the Payroll Department was in accordance with section 42 of the Act.
- The disclosure of employees' SINs on computer printouts of time sheets to staff in other departments was not in accordance with section 42 of the Act.
- Reasonable measures to protect computer printouts of time sheets in the departments were defined, documented and in place, in accordance with section 4(1) of Regulation 460 under the Act, as amended by Regulation 532/93.

- Reasonable measures were defined, documented and in place, to prevent unauthorized access to employee-related personal information stored in the hospital's computer systems in accordance with section 4(1) of regulation 460 under the Act, as amended by Regulation 532/93.

RECOMMENDATIONS

We acknowledged that the Ministry has amended its payroll procedures effective October 1993. All staff are now required to pick up their own pay cheques/pay stubs personally from the Business Office. It is the Ministry's view that this procedure has eliminated the need to seal pay cheques/pay stubs in sealed envelopes. We concur with this view.

We, therefore, recommend that the Ministry:

1. find an alternative method for collecting employees' time worked information that would not involve the disclosure of employees' SINs to staff of departments other than the Payroll Department.
2. remind staff of their obligation to follow Ministry procedures at all times with respect to the security of personal information contained in computer printouts of time sheets.

Within six months of receiving this report, the Ministry should provide the Office of the Information and Privacy Commissioner with proof of compliance with the above recommendations.

Original signed by: _____
Susan Anthistle
Compliance Review Officer

December 8, 1993 _____
Date