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

Personal Health Information Protection Act, 2004

REPORT

FILE NO. HI-050011-1

A Community Care Access Centre

Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9188
TTY: 416-325-7539
http://www.ipc.on.ca

Personal Health Information Protection Act, 2004

REPORT

FILE NO. HI-050011-1

INVESTIGATOR: Nancy Ferguson

SUMMARY OF INFORMATION GIVING RISE TO THIS REVIEW:

A Manager at a Community Care Access Centre (the CCAC) was unable to find her portable digital assistant (PDA). The PDA contained email and calendar functions which included information about CCAC clients. The CCAC reviewed its obligations under the *Personal Health Information Protection Act* (the *Act*) including the notification of the affected clients. The loss was reported to the Information and Privacy Commissioner/Ontario (the IPC).

RESULTS OF REVIEW:

The PDA was not password protected. It contained a cellular phone and had been stored in the Manager's purse. It was last seen the afternoon before she attended a work-related conference. She did not use it the day of the conference and first noticed it missing from her purse the next day. She undertook a search of her home and car and contacted the conference centre that evening, but was unable to locate the device. The next morning she tried dialing the phone number to see if she could hear it ring, but there was no response. She notified the CCAC's Privacy Officer, her manager and the Director of Corporate Services of the loss. Contact also was made with the conference organizing Committee to see if anyone had found the PDA device.

The PDA's network password was immediately disabled as was access to all folders, email, calendar and task functions. The PDA's account was deleted from the system to further prevent access. Bell Canada was also contacted and the phone number was suspended.

Since the same program containing the same information was installed on the staff member's office computer, CCAC staff reviewed the documents in the email and calendar functions on her desktop computer. Any document containing client information was printed and delivered to the

Privacy Officer. The list of clients identified in the email messages and on the calendar was determined for the purposes of notifying them of the loss.

The CCAC worked closely with the IPC to develop a letter providing notification of the loss to the affected clients. This notice set out how the loss occurred, described the information that was on the device and pointed out that the CCAC was reviewing its practices to try to prevent a similar incident from occurring in the future. Each client was advised that the loss was reported to the IPC and was provided with the contact information of the CCAC's Privacy Officer who was available to provide further information. Two of the affected clients were deceased. Notification of their estates was considered but not carried out given the circumstances of this case. Further, two individuals named on the PDA could not be determined with certainty to have been clients of the CCAC and as a result, were not contacted.

It was explained to all clients contacted that their information was only available on the device for the short period of time before the device's access was disabled. It was also pointed out that the device was likely of interest to someone because it contained a cellular telephone as opposed to someone interested in the personal information stored on the device.

Case Managers of the affected clients were informed that notification was taking place so they could effectively respond to any questions raised by the clients or other staff.

A copy of the letter providing notification was placed in each client's file.

To help avoid a similar incident from occurring in the future, all staff members carrying a PDA were notified to make sure they have a password with mixed characters and a minimum of 7 characters. They were advised to ensure this password is different from the password they use to log on to the network. Staff were also advised that any reference to clients in emails or other documents stored on the PDA should be made using only a unique identifying number or the client's initials.

The CCAC also decided that it would no longer enter the organization name and email address on the PDA; it would only provide a user name and the phone number for the device. It also advised staff that the PDA should stay with the staff member and be worn on the body and should not be left unattended in meeting rooms or in vehicles. Staff were also advised that the PDA is to be placed in a locked drawer in the office and not left on the cradle in plain view. All PDA's were also set to "power off" after 15 minutes of no activity. The CCAC is also exploring the use of encryption software for its PDA devices.

Staff at the CCAC have been advised of the steps to take if their PDA goes missing, including when the loss is detected outside of working hours. Staff were informed of the breach, of the actions that were taken by the CCAC in response, and about the resulting changes in policies and procedures. There was also a general review undertaken with staff concerning the privacy protection provisions of the *Act*.

On the basis of all of the above, it was determined that further review of this matter was not warranted and the file was closed.

Original Signed by: August 22, 2005

Ann Cavoukian, Ph. D.
Commissioner