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-050015-1

A Nursing Services Company

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-050015-1**

INVESTIGATOR: Nancy Ferguson

SUMMARY OF INFORMATION GIVING RISE TO THIS REVIEW:

A computer belonging to a small private company that provides specialized nursing services (the company) could not be found following a break-in. The company reported this matter to the police and the Office of the Information and Privacy Commissioner/Ontario (the IPC). The company also undertook a consideration of its obligations under the *Personal Health Information Protection Act, 2004 (*the *Act)* including notice to affected patients under section 12(2).

RESULTS OF THE REVIEW:

The IPC conducted a review of this matter and obtained the following information from the company.

The company reported that it provides specialized care primarily to individuals in their own homes and to patients in local hospitals and long-term care facilities. The company advised that the computer that was taken during the break-in contained a database with information about the individuals to whom it provided health care services. The database, which was used for billing, scheduling and statistical purposes, was not password protected.

The database contained information about individuals who had been referred to the company from a number of different sources, including:

- the local Community Care Access Centre (CCAC) for individuals receiving care at home;
- local hospitals for individuals who were in the hospitals; and
- local long term care facilities for individuals in these facilities.

The company advised that the majority of the affected patients were referrals from a Community Care Access Centre (CCAC). For these patients the computer's database included the patient's

name, address, phone number, date of birth and health card number. A diagnosis relating to the nursing service provided was usually included.

The company advised however, for the other individuals affected in this incident, the database contained less information. For example, for individuals who received the company's nursing services in hospitals and long term care facilities, the database would usually only contain the patient's name and the unit or department where they received services. The database did not contain addresses, phone numbers or health card numbers for these individuals. In some cases there was diagnostic information relating to the nursing service provided.

The company noted that although the database was not password protected, there was a back-up which permitted the company to access the information and identify the affected patients on its database. The company felt it was important to note that there were no nursing notes on the system, except for several letters to insurance companies providing health history and a request for funding for a particular type of treatment. Unfortunately, the word processing portion of the system was not backed up, so these letters could not be retrieved to determine the identities of the affected individuals.

The company reported that it had been in contact with the CCAC, the hospitals, the long term care facilities, the Workplace Safety and Insurance Board and the other nursing agencies that it provided services to, about the loss. The company agreed that it would keep these organizations informed about its consultations with the IPC concerning the notification of affected individuals.

The company worked closely with the IPC to develop a plan to carry out patient notification. This plan included the following:

- the creation of a notice indicating that a computer had been stolen and giving the contexts and the nature of the information on the computer for the clients in each of the settings;
- the notice indicated the IPC was contacted and was aware of the loss and offered a contact name and phone number for an individual at the company who could assist in responding to questions;
- the notice was forwarded to area physicians, the local hospitals, long term care facilities and other agencies likely to have clients receiving services of the nature provided by the company, including all area family physicians;
- local physicians, long term care facilities and other facilities and agencies likely to have continued contact with affected patients were asked to post a copy of the notice in their facilities, in a place likely to come to the attention of patients;
- these local physicians, long term care facilities and other facilities and agencies likely to have continued contact with affected patients were also asked to inform any patient they were aware had received care from the nursing company about the loss and refer them to the posted notice; and
- for the company's other clients/patients not referred by an outside agency, verbal notice will be provided to the affected individuals, who are current clients.

The company advised the IPC that it would be taking steps to better secure its database. This new approach will protect patient health data from unauthorized use. The approach involves physically separating patient identifying data from the clinical data contained in the database except when in use at the office during the day. The company advised that it also intends to create a method to "de-identify" the information on the database once the client is no longer receiving services.

The company reported the following with respect to increased physical security measures to avoid a similar loss in the future:

- locks were changed on the first entrance to the office as it appeared the office was entered with a key stolen from the landlord's office;
- the landlord advised that he would consider replacing the existing front door lock with a more secure access system; and
- a security alarm was purchased for the office.

The company indicated that, as a result of this incident, it had reviewed other issues relating to the management of personal health information. The company noted that its business involves the need to distribute information to nurses in the field, and the transport and storage of this information while nurses are working outside the office. For example, nurses receive information in their homes through faxes sent from the company's office. These nurses are frequently travelling and do not come to the office everyday since the service area covers a large geographical area.

The company reported it had undertaken the following improvements to address these issues:

- when faxing personal health information to nurses in their homes, for nurses who travel to see patients, a "fax on demand system" will be implemented to only permit the printing of faxes when the nurse is present to actually receive the information;
- The possibility of using encryption software will be explored when faxing patient personal health information;
- for nurses who do not come into the office everyday and who frequently travel to see patients, the company will implement document security bags that would be used for the daily transportation and storage of personal health information including one bag for daily transportation and a second to stay in the nurses home office, locked and secured;
- new privacy and security policies covering the management of personal health information will be implemented; and
- a training session was carried out with staff to increase awareness about the incident and the application of the *Act* to their work.

The company noted that its nursing agency colleagues were very interested in the solutions developed to better safeguard information in the course of community nursing.

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

Original signed by: December 19, 2005

Ann Cavoukian, Ph.D.
Commissioner