



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-050007-1

A Private Laboratory



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/Télé: 416-325-9188
TTY: 416-325-7539
<http://www.ipc.on.ca>

Personal Health Information Protection Act, 2004

REPORT

FILE NO. HI-050007-1

INVESTIGATOR: Nancy Ferguson

SUMMARY OF INFORMATION GIVING RISE TO THIS REVIEW:

A computer containing the personal health information of patients who had attended a private laboratory for diagnostic testing was found missing after a break-in at the lab. The lab reported the matter to the police and the Information and Privacy Commissioner/Ontario (the IPC). The loss was also brought to the attention of the Ministry of Health and Long Term Care (the Ministry) as the data on the computer included patients' Ontario Health Insurance Plan (OHIP) numbers. The lab worked with the IPC to address its obligations under the *Personal Health Information Protection Act* (the *Act*) including the notification of affected patients.

RESULTS OF REVIEW:

The computer was used to gather and store electrocardiogram (ECG) data and related patient health information including, for each patient tested, their name, address, birth date, treating physician, and relevant medical history.

The computer was a "stand-alone" with no connection to any network. The computer was owned and maintained by a private company that contracted with the lab to provide analysis of the diagnostic data. The computer was estimated to contain two and a half years of data; and unfortunately, there was no back-up of the information that was stored on its hard drive. These factors made identifying the number of patients affected and determining their contact information very difficult.

The IPC worked closely with the lab to develop a notification program to fit the circumstances of the loss and reach as many patients as possible pursuant to its obligation to provide notice under section 12(2) of the *Act*. The program agreed upon provided for the following:

1. A Letter to Area Physicians enclosing a Public Notice

The lab prepared a list of all area family physicians and some cardiologists who regularly sent clients for ECG testing. The lab sent each physician a letter advising them of the loss, and requesting that they post in their office a "Public Notice" describing the incident for patients. They were also asked to deliver a copy of the Public Notice to patients believed to have been affected, based on the information provided.

With the agreement of the Ontario Medical Association (the OMA), the lab included a statement in the letter to the physicians indicating the OMA was supportive of the doctors helping to make patients aware of the incident.

The Public Notice describes the theft and the address of the lab where the theft took place. It indicates that the theft was reported to the police and provides a description of the type of patient information that was on the computer. The notice refers to contact with the Ministry of Health and the IPC and provides contact information for patients wishing to obtain further information from the lab.

2. Posting a Public Notice at the Lab Where the Theft Occurred

The lab posted a copy of the Public Notice at its facility. This aspect of the notification program was considered important given the particular type of diagnostic testing involved in that there was significant potential for affected patients to return to the lab for further testing. Patients receiving ECG testing often attend for follow-up ECG testing to monitor their status.

3. A Press Release to Local Media Outlets

The lab also created a news release which it delivered to local print and radio press outlets. The press release contained similar information to that set out in the Public Notice.

In addition to its own internal investigation to identify the scope of the loss of personal health information arising from the incident, the lab indicated it would conduct an impact assessment to help identify further risks of health information loss. The lab also indicated that necessary preventative protocols would be implemented including taking steps to ensure data is properly backed up, securely stored and deleted from the computer used to collect the diagnostic data. Password protection was implemented for all computers at the lab and a monitored security alarm system was installed.

The lab also determined that it would need to develop, execute and implement a data sharing agreement with the private company that was involved in the supply of the computer and the diagnostic analysis of patient test data.

The lab agreed to consult with the IPC's Policy & Compliance Department as it puts in place the data sharing arrangement and implements other policies and procedures required to comply with the *Act*.

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

Original signed by: _____
Ann Cavoukian, Ph. D.
Commissioner

July 4, 2005 _____