Personal Health Information Protection Act, 2004

REPORT

FILE NO. HI-040001-1

A Hospital in a Rural Centre

Personal Health Information Protection Act, 2004

REPORT

FILE NO. HI-040001-1

INVESTIGATOR: Nancy Ferguson

SUMMARY OF INFORMATION GIVING RISE TO THIS REVIEW:

A hospital advised that two computers went missing from the physiotherapy department. The computers were discovered missing by staff. There was no sign of forced entry. The hospital was faced with how to fulfill its obligations under the *Personal Health Information Protection Act* (the *Act*) including the notification of affected patients. The hospital reported the loss of the computers to the police and the Information and Privacy Commissioner/Ontario (the IPC).

RESULTS OF REVIEW:

The hospital's network was password protected, however, the hard drives of the two computers that went missing were not. The two computers had only been in use for six months. There was no way to confirm exactly what patient information was stored on the computers. It was discovered that administrative staff had a practice of saving any document containing patient information to the network. However, the clinical staff reported not using this practice on every occasion. The hospital asked each staff member in the department to describe their use of the computers and to recall what they had saved on them.

From these discussions with staff it was determined that the computers were used almost exclusively to prepare "progress notes" to describe the services provided to patients. These notes indicated the patient's full name and described the reason the patient was seeking services, the services provided and the outcome for each patient. The computers also contained a list of patient names indicating each patient's full name and "ward" within the hospital.

Section 12(2) of the *Act* requires "Health Information Custodians" to notify patients if their personal health information is stolen, lost or accessed by unauthorized persons. In this case, the hospital undertook verbal notification of each patient whose "progress note" was believed to be on the computer. The hospital also undertook verbal notification of each patient whose name was found on the list of patients.

With the assistance of the IPC, the hospital structured a notification document outlining what each patient should be told to fulfill the *Act's* notification requirement.

Patients were contacted using information the hospital had on file. The notification process included providing each patient with an outline of what happened and a description of the steps taken by the hospital to contain the situation. Patients were told the police were contacted and that the computers were not recovered. Patients were also advised that the hospital was working with the IPC to ensure they were meeting all the requirements under the *Act* and offered contact information for the IPC. The notification process was substantially completed with only a few individuals remaining to be informed. The hospital is continuing to work on establishing contact with these patients to convey notification.

The hospital implemented several measures to reduce the risk of a similar situation occurring in the future. Staff within the department, and all staff at the facility dealing with patient information on computers, were advised not to save personal health information on local hard drives. Department managers were asked to check computers to ensure patient information was removed from local hard drives. The hospital requested its computer support personnel to put a system or program in place that would result in documents from certain applications being saved as a default to the network. The idea being that this would encourage and remind staff that documentation should be saved to the network because it would automatically direct them to the network each time a document was saved. The facility is also considering the best approach to ensure new staff are informed about the importance of not saving patient information to local hard drives.

The hospital also undertook some changes relating to the physical security in place to help prevent computers from being stolen. Locks were changed in the department where the loss occurred and new keys were distributed and recorded.

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

March 22, 2005

Ann Cavoukian, Ph.D.
Commissioner