



Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

Personal Health Information Protection Act

REPORT

FILE NO. HR06-53

A Hospital in an Urban Setting



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

REPORT

FILE NO.

HR06-53

INVESTIGATOR:

Cathy Hamilton

HEALTH INFORMATION CUSTODIAN:

A Hospital in an Urban Setting

SUMMARY OF INFORMATION GIVING RISE TO REVIEW:

The Privacy Manager at a hospital contacted the Office of the Information and Privacy Commissioner/Ontario (the IPC) to advise that, on three separate occasions, clerical staff (clerks) on three different units in the hospital inappropriately accessed the personal health information of a total of seventeen patients. The IPC opened a file and worked with the hospital to fulfill its obligations under the *Personal Health Information Protection Act* (the Act).

RESULTS OF REVIEW:

The hospital's Privacy Manager conducted an internal investigation upon learning of each incident, and provided the following information to the IPC.

In the first incident, audits of two deceased patients' electronic patient records (EPR) showed that a clerk had accessed their EPRs. There was no clinical relationship between the clerk and the deceased patients. Further audits were run on the clerk's access to EPRs and it was discovered that the clerk had also accessed the EPR of a family member.

In the second incident, an audit conducted on a clerk's access to EPRs showed that the clerk had accessed the EPRs of thirteen patients with whom there was no clinical relationship. The patients whose EPRs were accessed were the clerk's current family members, her ex-spouse's sister, her boyfriend, and members of her boyfriend's family.

In the third incident, a clerk arrived in the hospital's emergency department after learning, through the EPR system, that the clerk's friend had been admitted to the emergency department. The clerk did not have a clinical relationship with the patient.

In all three incidents, the hospital took immediate action to respond to the unauthorized access of patients' personal health information. The Privacy Manager conducted internal investigations and all three clerks were subject to disciplinary action.

With respect to the notification requirements under section 12(2) of the *Act*, the hospital fulfilled its obligations, as the Privacy Manager had already notified the affected individuals and/or their substitute decision makers prior to reporting the incidents to the IPC. All individuals were notified in writing of the privacy breach and were provided with the Privacy Manager's name and contact information in the event they had any questions.

As a result of the similar nature of the incidents, the hospital conducted a review of its policies and procedures that relate to the privacy of personal health information. The hospital had a number of existing policies in place relating to the privacy of personal health information, including one policy applicable to staff that specifically indicated that an unacceptable use of information technology resources includes "accessing electronic records of patients or employees where access is not required to perform the duties for which an individual is employed by or affiliated with the organization, including the user's own records and those of family and friends."

In addition, the hospital is in the process of developing a policy on the access and disclosure of personal health information and a policy/protocol on the steps it will take in the event of a privacy breach. The hospital is developing the privacy breach policy/protocol using its expertise and the IPC's paper entitled "*What to do When Faced with a Privacy Breach: Guidelines for the Health Sector*," has provided a draft copy of it to the IPC and will notify the IPC when the policy is finalized.

Lastly, the hospital's Privacy Office and communications department are in the process of developing a "privacy blitz" that it will conduct for all staff members that have access to personal health information. The "blitz" will consist of written materials and education sessions on the importance of a culture of privacy with respect to personal health information. For example, personal health information should not only be kept confidential, but in many circumstances should not be accessed at all.

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: _____
Brian Beamish
Assistant Commissioner

January 23, 2007