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-050013-1

A Hospital in an Urban 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-050013-1

INVESTIGATOR: Nancy Ferguson

SUMMARY OF INFORMATION GIVING RISE TO THIS REVIEW:

A hospital reported that a staff member had inappropriately accessed a patient's personal health information. The access was discovered as part of a routine audit by the clinical information system used in the hospital's Mental Health Department. The staff member did not work in the department but the audit indicated she had accessed the same patient's chart on several occasions. The hospital reviewed its obligations under the *Personal Health Information Protection Act* (the *Act*) including the notification of the affected patient.

RESULTS OF THE REVIEW:

The hospital reported that it makes a significant effort to limit access to patient information to those that properly should have it to perform their jobs. Employees are assigned security access based on the requirements of their job. Jobs with similar requirements are grouped together for the purposes of defining and testing a security profile. This profile is then assigned to each employee within the group.

The hospital noted that employees within hospitals very often move from department to department and cover shifts in different units or departments. This presents a challenge when trying to properly restrict access to patient information as it is very important that employees have the information they need to perform their work.

The hospital determined that, while its system allows for the management of a complex security profile designed to limit access except as appropriate, they also must rely on employees' respect for patient privacy and confidentiality, and adherence to privacy laws. The hospital noted that it works with employees to ensure they understand these responsibilities and requires each employee to sign an agreement setting out their obligations with respect to maintaining the

confidentiality of patient information. Training is also provided as part of the orientation process for new employees. The ability to audit access to patient records is another method to check that patient information is properly accessed and secured.

The hospital's *Privacy Policy* and *Privacy Procedure for Complaints and Investigations* set out that audits can be requested by patients, managers and physicians to determine who has accessed a patient's health information. Every month, three random audits are performed through the clinical information system used by the hospital. It was through this audit process that this breach was detected.

The hospital examined how the staff member was able to access the information of a patient that was not within the department where she worked given that the system was designed to limit such access. It was determined that this employee's access was initially limited to those patients receiving care in the department where she worked. Her access was eventually expanded to permit access to the information of all hospital patients because she was required to work in several departments at once. When she resumed working primarily in one department, her security profile was not modified because she was still occasionally required to cover shifts in other departments.

The staff member had signed a confidentiality agreement when she was hired and confidentiality had been discussed with her, as evidenced by the orientation checklist signed by the Manager and the employee in the summer of 2004. The hospital indicated that the staff member had not attended training sessions or staff meetings when the Privacy Policy was implemented. However, numerous articles had been published in the hospital newsletter and these were available to staff. The hospital also noted that an attachment to staff member's payroll stubs described the ten privacy principles underlying the privacy requirements.

In responding to the incident, the hospital immediately removed the access rights of the employee pending further investigation and suspended the employee with pay. The employee was interviewed and admitted to having looked at the patient's information for purposes unrelated to the delivery of healthcare services. The employee said she had not disclosed the information to anyone and had not accessed other patients' charts inappropriately. The hospital did not provide any information about the employee's motive for accessing the information.

The hospital reported that it has since identified other suspected breaches by this employee and is continuing its investigation. Ultimately, the hospital concluded the employee had committed a serious breach of confidentiality and dismissed the employee on this basis. The appropriateness of this dismissal is being disputed by the employee and her Union. The hospital indicated that arbitration is anticipated.

The patient whose information was accessed was provided with notice of the incident and advised of her right to complain to the IPC. The hospital ensured follow-up care was provided to the patient. The patient indicated she was satisfied with the investigation and did not wish to make a complaint to the IPC. The hospital has indicated that if other instances of unauthorized access of this patient's health information are detected through its ongoing investigation, the patient will be notified using the same process.

The hospital reviewed its Privacy Policy and procedures and determined there was no need to change them at this time. The hospital sets out, in its policy statement entitled "Confidentiality" that, as a condition of engagement, all staff, board members, volunteers, students and agents must review the policies regarding access and confidentiality and sign the confidentiality agreement before they obtain access to any patient information. The policy sets out a detailed definition of what constitutes a breach of confidentiality including:

"…Accessing patient or health information when it is not required to provide care to a patient or in the performance of duties. Examples of access considered to be a breach of confidentiality include:

- Accessing the health record of oneself other than through the documented Privacy Procedure…
- Accessing the health record of a staff member, family member, friend, or anyone for whom you do not have a requirement to view information based on providing care or performing duties
- Accessing any patient information (address, date of birth, next of kin, etc) for staff members, family member, friend or anyone for whom you do not have a requirement to view information based on providing care or performing duties."

The hospital noted that it had reviewed the recent activities it had undertaken in relation to staff education and system security and was satisfied. These activities included:

- appointing a Privacy Officer;
- establishing privacy teams at various levels of the organization to design, implement and manage changes to the information system;
- developing, implementing and training staff regarding the Privacy Policy and associated procedures;
- setting up security groups in the system used to manage patient information to limit access by staff to that required for their job and other security according to the Privacy Policy;
- updating the patient registration procedure and providing training for all registration/intake staff;
- reviewing the Confidentiality Policy in collaboration with Union groups and revising it as necessary and having staff, physicians, volunteers and vendors sign the agreement as revised;
- placing privacy posters strategically throughout the hospital to inform patients of the purposes for which their personal health information is collected, used and disclosed and for viewing by staff, volunteers and the general public;
- developing and implementing a public awareness campaign which included an article in the local newspaper and an interview with a local television program which was repeatedly broadcast over a one week period;
- Conducting 23 educational sessions about the *Act* and offering them at different times to accommodate shift workers at all the hospital's sites, and advertising them in departments and the hospital's newsletter;

- Providing training at staff meetings and skills fairs and one on one with staff;
- Providing information about privacy and confidentiality and the *Act* specifically through the hospital's newsletters and information attached to payroll stubs, and through the intranet and articles circulated to particular departments;
- Revising staff and volunteer orientation policy and checklists to strengthen the confidentiality section and developing a physician orientation policy;
- Discussing whiteboards and the other posting of patients' names on walls with managerial staff and program directors and all staff at staff meetings and education sessions;
- Implementing audit procedures to check on the proper use of patient information by staff.

The hospital stated that these were the activities undertaken in relation to staff education and system security but noted the implementation of the hospital's Privacy Strategy included many other activities.

In relation to this particular incident, the hospital indicated that it planned to reinforce the need for confidentiality with its managers, staff, physicians and volunteers. This was accomplished by mailing a reminder to all staff relating to the importance of privacy and security of patient information. In addition, the Privacy Officer will meet with all managers to remind them of their responsibilities relating to the security of patient information.

To help avoid a similar incident going forward, the hospital will continue with its education of staff, continue with its audits and continue to send email, internal newsletters and other materials to remind staff of their obligations.

The hospital will also ask the managers of each department to review the security privileges of each of their employees to ensure their employees do not have more access than is required to perform their work. An exception report will be created to help assess if certain employees have more security privileges than they require.

A project team will be created to review security profiles for employees based on job functions. The hospital will also create a review process to track changes made to security profiles for groups or individuals. A process will be established to grant exceptional security access (not based on job function) that requires signature by Physician or Director level staff. The hospital has also determined that a new process needs to be developed to better manage the "transient" nature of its staff as employees cover one another for shifts. New profiles will be assigned to all employees based on their job functions and regular review of these profiles will be carried out. Further, all individual security profiles will possess an end date to ensure regular review of each staff member's profile.

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 29, 2005

Ann Cavoukian, Ph. D.
Commissioner