Hôpital Montfort

Q. What type of information was found on the USB key?

The USB key contained information such as the name of the patient, the type of service they received and the dates involved, as well as a special code that is linked to the health service provider.

Fortunately, no other personal or health information was included on the USB key: no health card number, no diagnostic notes, no postal address, no financial information were included in the file.

Q. How many patients were involved?

Approximately 25 693 patients.

Q. When was the key lost?

The key was lost on November 24 and reported lost on November 26, 2012.

Q. Why was there a six week delay before contacting patients?

As soon as the incident was reported, the hospital took measures to reconstruct the data contained in the files and compile a report to determine the type of information contained on the key and the risks attached to such information. A letter was prepared and a firm was hired to perform the mail-out. Given that no demographic information was associated with the patient name on the USB key, we then had to match the right name to the correct address to send the letter to the right patient.

Q. How is it possible that confidential information was found on an unencrypted USB key?

This is one of those unfortunate unauthorized incidents that act as a catalyst for the hospital to conduct an immediate and thorough review of its policies and to underscore to all of our employees just how important it is to protect the confidentiality of all patient information.

Q. What is Montfort's policy concerning the protection of patient privacy?

The hospital has several policies in place concerning the security and protection of personal health information. The two major ones have to do with confidentiality in the broad sense of the term (personal information, personal health data, administrative information), as well as a policy that is specifically related to personal health information.

Q. Has disciplinary action been taken?

Montfort has worked very hard to cultivate a workplace where fairness and transparency are of utmost importance. We encourage all our employees to admit to their mistakes and declare incidents so that we can learn from them and put new systems in place to help ensure that these or similar mistakes don't happen again – for the employees involved as well as for others.

Hôpital
Montfort

Q. Have you contacted the people whose information was on the USB key?

Yes, in the interest of full transparency, the patients whose names were included on the USB key have received a letter from the hospital explaining the incident. They were invited, if they so desired, to contact our privacy protection personnel.

Q. What measures were taken to avoid that such an incident does not repeat itself in the future?

The hospital has implemented a concrete plan of action that includes a full review of policies and procedures. Our information systems and security measures for mobile devices have also been modified in order to minimize the risk that such an incident can repeat itself in the future.

For the longer term, we will ensure that high security standards will be put in place to protect personal information and we will engage in training programs for staff members with respect to patient confidentiality. We will also engage in an audit of our practices regarding the use of mobile devices.

Q. Have you advised the Ontario Privacy Commissioner?

Yes. We have notified the office of the Privacy Commissioner in order to receive their advice and to assure our patients of full transparency on this matter.