



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. HR07-36

A Mental Health Facility

---

---



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.**

**HR07-36**

**INVESTIGATOR:**

**Cathy Hamilton**

**HEALTH INFORMATION CUSTODIAN:**

**A Mental Health Facility**

### **SUMMARY OF INFORMATION GIVING RISE TO REVIEW:**

The Privacy Officer of a health information custodian (custodian), a mental health facility, contacted the Office of the Information and Privacy Commissioner/Ontario (the IPC) to report that a laptop containing personal health information had been stolen from a staff member's vehicle. The IPC opened a file and worked with the custodian to fulfill its obligations under the *Personal Health Information Protection Act* (the Act).

### **RESULTS OF REVIEW:**

The custodian's Privacy Officer provided the IPC with the following information.

The staff member worked at two satellite locations of the facility and was provided with the laptop to facilitate her mobility between the two locations. The laptop may have contained the personal health information of up to approximately 590 individuals, and may have included some or all of the following information: the individual's name, age, telephone number, planned assessment date, referral source, medication use, substance use status, diagnosis, health history, past/current therapy support, history of hospitalizations, probation status, employment status, living arrangements, disability/social assistance, attendance at outpatient groups, and casebook number.

The individuals whose personal health information was stored on the laptop fell into one of three categories: active inpatients/outpatients; inactive patients; and individuals who were referred to

the custodian, but never admitted as patients. In addition, a very small number of the inactive patients were deceased.

The laptop, although password protected, was not encrypted.

The staff member involved reported the theft immediately to her Manager and to the local police. The following day, members of the custodian's leadership team were notified of the theft, and its Information Technology staff immediately disabled remote access from the laptop to its network. In addition, the custodian confirmed that no personal health information was permanently lost, as it was also saved either on the network or archived in hard copy.

As a result of the incident, the custodian replaced the laptop with desktop computers at each of the satellite locations. In addition, the custodian sent a written reminder to staff regarding its policies on the security of personal health information and computer use, implemented mandatory strong password changes for all computers, and provided mandatory laptop clinics for all staff using laptops.

With respect to the use of encryption, the custodian collaborated with other health information custodians to evaluate, purchase and implement encryption software for its laptop computers. The software has been purchased and will be implemented over the next few months.

With respect to the notification requirement under Section 12(2) of the *Act*, the custodian advised the IPC that due to the affected individuals' diagnoses and poor coping skills, they comprised a particularly vulnerable group who may present a significant risk of harm to themselves or others upon notification of the privacy breach, in the absence of clinical support.

Therefore, the IPC worked closely with the custodian to determine the most appropriate method of providing notification. Subsequently, the custodian notified those individuals who were active inpatients/outpatients, those inactive patients and those previously referred but not admitted as patients, who have since presented to the facility for assessment, in person, via the treatment team. With respect to the remaining individuals, the custodian agreed to send notification letters to the individuals' referral source and/or follow up health care provider. In the letter, the custodian will ask the health care provider to notify the patient of the privacy breach at the next visit, and provide the custodian's contact information should any questions or concerns arise.

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.

October 2, 2007

---

Brian Beamish  
Assistant Commissioner