

ENCRYPT ELECTRONIC HEALTH RECORDS

Ontario Commissioner Gives Health Care Custodians Strict Guidelines

What Happened?

A physician at Toronto Hospital for Sick Children (Sick Kids), who also functions as a researcher there, left the hospital on January 4, 2007, taking one of the hospital's laptop computers, with the intention of analyzing the research data stored on it at home. However, he did not go directly home. The physician parked his minivan in a downtown Toronto parking lot between 7:30 and 11 p.m., leaving the laptop under a blanket between the front seats of the van (which had no trunk). When he returned, he discovered that the front passenger window had been broken and the laptop had been stolen.

The personal health information stored on the stolen laptop included 2,900 patients' names and individual Sick Kids numbers as well as information relating to the patients' medical conditions.

In some cases, very sensitive information was also included such as drug therapy and HIV status. The health information of the patients was being used in 10 different research studies. Some of the patient information had been provided to Sick Kids by the University Health Network (UHN), since roughly 350 of the patients had been treated at both Sick Kids and UHN.

All of the data on the laptop was also saved on the Sick Kids' main server, but the only security measure on the laptop was a login password.

Ontario Information and Privacy Commissioner Ann Cavoukian¹ has ordered Sick Kids to introduce a number of specific protections. The most notable measure required is the need to encrypt any personal data taken out of the hospital on a laptop or other remote computing device.

Among the provisions in the

- Sick Kids must develop and implement a comprehensive corporate policy that prohibits the removal of identifiable personal health information in electronic form from the hospital premises. In the event that personal health information in identifiable form needs to be removed in electronic form, it must be encrypted.
- The hospital must also develop and implement a hospital-wide endpoint electronic devices policy, applicable to both desktop and portable devices (laptops, PDAs), which mandates that any personal health information not stored on secure servers must either be de-identified or encrypted.

Going further, the Commissioner is telling all health information custodians in Ontario that they should never store any personal health information on their laptops or mobile computing devices unless they have taken strong steps (such as encryption) to ensure that the information is protected against unauthorized access, if the device is lost or stolen.

Commissioner Cavoukian provided guidance to all health information custodians on how to protect personal health information. Where personal health information must be stored on portable electronic devices, only the minimal amount of information necessary should be stored, and for the least amount of time necessary to complete the required work. Most importantly, where personal health information is stored on mobile devices in identifiable form, the information **must** be encrypted, said Commissioner Cavoukian. “At a minimum, files or folders containing personal health information must be encrypted. It is essential to use up-to-date encryption techniques to ensure that personal health information is appropriately secured.”

The Commissioner is “strongly urging” all health information custodians to regularly review their privacy and security policies and procedures relating to the storage of health information on mobile computing devices to ensure that they, “are effective in minimizing the significant risk to privacy posed by the loss or theft of such devices.” This message is particularly timely in light of the present month, March, being recognized as Fraud Prevention Month.

“All health information custodians,” said Commissioner Cavoukian, “should invest in proactive measures to protect personal health information stored on mobile computing devices. In the event that such a device is lost or stolen, this would save custodians time and money by allowing them to avoid the notification requirements of *PHIPA*, as well as protecting individuals from the undue stress of knowing that their personal health information was lost or stolen. It will also prevent the potentially irreparable damage to a custodian’s reputation resulting from the loss or theft of health information from their hospital or office.”

The “Commissioner’s Message” contained in the Order ends with: “There is no excuse for unauthorized access to personal health information (PHI) due to the theft or loss of a mobile computing device – any PHI contained therein must be encrypted.”

The Commissioner’s health order is available at: www.ipc.on.ca.

Media contact:

Bob Spence

Communications Co-ordinator

Office of the Information and Privacy Commissioner/Ontario,

Phone: 416-326-3939

Cell: 416-873-9746

bob.spence@ipc.on.ca

ⁱ 07-03-08 Health order (HO-004) issued under the Personal Health Information Protection Act (PHIPA).