



Information and Privacy
Commissioner/Ontario

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

News Release

January 14, 2010

Commissioner Cavoukian Orders Durham to Encrypt Health Information on all mobile devices: calls for immediate action to prevent any more “unacceptable” breaches in Ontario

TORONTO – Ontario Information and Privacy Commissioner, Dr. Ann Cavoukian, today ordered Durham Region’s Medical Officer of Health to ensure that all personal health information stored on mobile devices is strongly encrypted. A health order issued by the Commissioner addresses a recent privacy breach in Durham Region, but also goes beyond to focus on the province-wide issue of protecting personal health information stored on mobile devices.

Commissioner Cavoukian’s Office conducted an in-depth investigation following the loss of a USB key, reported to her office on December 21, containing the personal information of nearly 84,000 people who had attended H1N1 immunization clinics in Durham Region.

As the “health information custodian” ultimately responsible for the unencrypted memory stick that was lost, Dr. Robert Kyle, Durham’s Medical Officer of Health, was ordered to immediately implement procedures to ensure that any personal health information stored on any mobile devices (laptops, memory sticks, etc.) is strongly encrypted.

Commissioner Cavoukian also made it very clear that she expects **all** personal health information stored on any type of mobile device in Ontario to be protected with strong encryption.

“While I accept that custodians may not be able to totally eliminate the loss or theft of mobile devices, what I cannot accept is that the information contained therein is not encrypted,” the Commissioner stated in the Order. “Unauthorized access to health information stored on these devices that happen to be lost or stolen may clearly be prevented through the use of encryption technology. However, despite strong incentives to avoid privacy breaches and the availability of encryption to prevent such breaches, unencrypted mobile devices continued to be used. This is both distressing and completely unacceptable.”

Commissioner Cavoukian reminded health information custodians of their obligations under Ontario’s *Personal Health Information Protection Act (PHIPA)*, with specific focus on the issues raised three years ago in HO-004, a health order the Commissioner issued in 2007, and more recently, HO-007. Both of these Orders deal with the loss of unencrypted personal health information, of thousands of people.

The Commissioner also ordered that Durham Health cease the collection of specific types of information at Durham H1N1 immunization clinics, namely health card numbers and (unless it becomes pertinent in the future), personal health information pertaining to priority group status.



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9195
TTY: 416-325-7539
<http://www.ipc.on.ca>

To ensure that practices at public health units across the province comply with *PHIPA*, Commissioner Cavoukian also directed recommendations to the Ministry of Health and Long-Term Care, including:

- that each of the 36 health units in Ontario conduct a review of its practices and procedures with regard to the encryption of mobile devices in order to ensure that any personal health information on those devices is strongly encrypted;
- that the ministry receives an attestation from each medical officer of health in the province that no unencrypted personal health information is being transported on mobile devices, and that the ministry conducts audits of a representative sample of public health units, to verify the information; and
- that training materials be developed to ensure that all public health unit staff are aware of the need for proper safeguards for personal health information stored on mobile devices.

“I believe that in light of the proliferation of new information and communication technology, the future of privacy requires a comprehensive and proactive *Privacy by Design* approach, whereby both privacy and security are effectively built into the information eco-system, from end-to-end, and throughout the entire data lifecycle, from collection through to disposal,” said the Commissioner.

Durham Region is already moving quickly to address the Commissioner’s concerns, after meetings held during her office’s investigation into the incident. “My office has met with the Durham Health Unit and confirmed that there will be no further storage or transportation of patients’ information on USB sticks that are not encrypted,” said the Commissioner. “We have also confirmed that Durham Region has taken decisive steps to implement privacy-protective solutions for all mobile devices (beginning with its health unit) in the form of strong encryption technology from CryptoMill Technologies, an Ontario company that specializes in protecting the privacy and security of data on laptops, desktops and all mobile storage devices.”

For a copy of the Order, visit www.ipc.on.ca

The Information and Privacy Commissioner is appointed by and reports to the Ontario Legislative Assembly, and is independent of the government of the day. The Commissioner’s mandate includes overseeing the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*, as well as the *Personal Health Information Protection Act*, which applies to both public and private sector health information custodians. The Commissioner’s mandate also includes helping to educate the public about access and privacy issues.

Media Contact:

Bob Spence
Communications Co-ordinator

Direct line: 416-326-3939
Cell phone: 416-873-9746
Toll free: 1-800-387-0073
bob.spence@ipc.on.ca