



GARDINER ROBERTS

PRIVACY COMMISSIONER'S ORDER RESPECTING BREACH IN DURHAM REGION:

A DIRECTIVE FOR HEALTH INFORMATION CUSTODIANS *PRIVACY COMMISSIONER ORDERS ENCRYPTION OF PHI ON ALL MOBILE DEVICES; RECOMMENDS AUDITS, TRAINING, POLICIES TO PROTECT PHI*

THE BREACH

In December 2009, the Regional Municipality of Durham (the "Region") operated eight community clinics to provide the H1N1 vaccine to residents. The clinics were operated by public health nurses working for the Region. Individuals who attended the clinics were asked to provide personal health information ("PHI") including their names, addresses, dates of birth, health card numbers and additional health information. This information was collected and stored on USB memory sticks – memory sticks that were not encrypted. One such memory stick contained the PHI of 83,524 individuals who attended H1N1 immunization clinics in the Region. A public health nurse employed by the Region discovered that she had lost the memory stick as she walked from the main building of the Region's headquarters to her car in the parking lot.

When the missing memory stick could not be located, the Region's Medical Officer of Health, who was also its Health Information Custodian ("HIC"), advised the Information and Privacy Commissioner of Ontario (the "IPC") of the loss and engaged the IPC in managing and reporting of this breach. The incident made headlines throughout Ontario and resulted in an immediate response: the IPC told all Medical Officers of Health in Ontario to immediately cease storing PHI on mobile devices unless they have strong encryption in place; and the IPC issued a news release directing Ontario's health sector to do the same, noting that this was required in a previous order of the IPC.

LESSONS (THAT SHOULD HAVE BEEN) LEARNED FROM PAST ORDERS

Central to the IPC's order¹ in respect of this breach (the "Order"), was the fact that a previous order of the IPC² (the "Sick Kids Order") directed that PHI be encrypted whenever it is stored on mobile devices. The Sick Kids Order was issued in March 2007 following the reported theft of a laptop containing PHI of thousands of patients of the Hospital for Sick Children. The computer was stolen from a physician researcher's minivan. While the information on the computer was password-protected, it was not encrypted. The IPC found that the Hospital for Sick Children, as a HIC, had failed to:

- take steps that were reasonable in the circumstances to ensure that the PHI in its custody or control was protected against theft, loss and unauthorized use or disclosure³; and
- ensure that the records of PHI in its custody or under its control are retained, transferred or disposed of in a secure manner⁴;

Gardiner Roberts LLP

Barrister & Solicitors
Scotia Plaza
40 King St. West
Suite 3100
Toronto, ON
M5H 3Y2

Tel: 416-865-6600
Fax: 416-865-6636

www.gardiner-roberts.com



This article was prepared by Lonny Rosen. Mr. Rosen is a partner in our health law department and can be reached at 416-369-4345 or lrosen@gardiner-roberts.com



In the “Commissioner’s Message”, contained at the conclusion of the Sick Kids Order, the IPC communicated to all HICs:

*...it is my view that it is no longer reasonable to store PHI on mobile computing devices, unless steps are taken to ensure that any PHI stored on such devices is protected against unauthorized access, in the event that the device is lost or stolen.*⁵

The IPC considered the breach in Durham in light of the Sick Kids Order, and the IPC’s communications since then regarding the importance of encryption as a means to safeguard PHI⁶.

THE FINDINGS

The IPC found that an employee of the Region distributed memory sticks for use by staff of the Region’s Health Department. **This employee was not aware of the requirement for encryption** of PHI stored on mobile devices. However, like the public health nurses and other employees who deal with PHI for the Region, **he was an “agent” of the HIC and was therefore expected to be aware of, and to take, the steps necessary to safeguard PHI Records**⁷.

The IPC found that the Region collected more PHI than was necessary to administer the H1N1 immunization program.⁸

The IPC also mentioned that the Region did not consult the IPC regarding its system for data collection that was developed by the Ministry of Health and Long-term Care (the “Ministry”) and Niagara Health Unit. While there is no such obligation to consult the IPC, the Order clearly implied that the IPC should have been engaged in the implementation of a storage system that is being used by 30 of the 36 public health units in Ontario. The IPC found that, by allowing the storage of PHI records on memory sticks, the HIC failed to ensure that PHI in its custody or control was retained, transferred or disposed of in a secure manner. Therefore, the HIC had failed to take reasonable steps to safeguard the PHI⁹.

The IPC similarly found that **the HIC failed to have information practices in place that comply with PHIPA requirements**. In particular, the relevant policy of the Region’s health department was dated April 2002, entitled PC/Desktop Security. It was in the process of being updated to address information storage on laptops and mobile devices, but the update had not been completed before the H1N1 immunization clinic was opened.

Finally, the IPC found that the HIC had failed to ensure that all agents were adequately trained with respect to appropriate safeguards for PHI¹⁰. The IPC stated:

I must stress that the Act requires more than simply the development of policies and procedures. It also requires that health information custodians ensure that the requirements of the Act are understood and implemented by all applicable staff members – “walking the talk” is critical. [emphasis added]



WHAT THE REGION DID RIGHT

The Order sets out the HIC's failures but also commends for a number of things it did right, including:

- Informing patients of the loss of their PHI¹¹
- **taking its PHIPA obligations seriously**, as evidenced by the planned use of virtual private network ("VPN") systems for storing and accessing PHI records (although these systems proved unworkable or unavailable, which resulted in the use of memory sticks as a stop-gap measure)
- **posting a privacy statement** at all registration areas, which statement was read to each individual prior to the collection of his or her PHI
- **informing** patients that they were **not obliged to provide all of the information requested** in order to receive their immunization
- **training staff with respect to PHIPA**¹² (although this training occurred for all staff in 2007 and the employee who provided unencrypted memory sticks was a relatively new employee who had not received this training)
- **having staff acknowledge their obligations** under PHIPA
- immediately **switching to a paper-based system** as soon as the breach was found to have occurred, and then using ready-to-deploy encryption software provided by the IPC
- immediately **engaging a security firm** to develop suitable encryption for PHI records
- **updating the Region's policies** regarding the storage of PHI so that these now conform with the reality of mobile devices

THE ORDER

The IPC ordered the HIC to:

1. **Immediately implement procedures** to ensure that PHI records are safeguarded at all times, specifically by ensuring that any PHI stored on mobile devices is strongly encrypted.
2. **Revise its written information practices** in order to comply with PHIPA and to consult with the IPC prior to finalizing those information practices.
3. Take the necessary administrative steps to ensure that H1N1 immunization clinics **cease collection of PHI beyond that which is necessary**.
4. Take the necessary administrative steps to **ensure that records** of PHI that should not have been collected (relating to priority status or health card numbers) **are securely destroyed**.



WHAT THIS MEANS FOR HICS

There is no question that **the Order applies to all HICs**. One can expect the IPC to have even less patience now for HICs who make the mistakes that the Medical Officer of Health of the Region was found to have made. It is therefore imperative that all HICs assess their risk of non-compliance by:

1. **Audits.** Undertaking comprehensive reviews of their information and privacy practices to ensure that the PHI they maintain is appropriately safeguarded.
2. **Training.** Ensuring that all staff who collect or use PHI are trained with respect to their obligations under PHIPA.
3. **Policy Review.** Ensuring that adequate policies are in place, which reflect the current practices of the HIC and its agents, and that the HIC and all of its staff are complying with their policies and procedures.

In other words, HICs must ensure that they, and their agents, are “walking the talk”.

By failing to do so, HICs are at risk of being the subject of a similar order and of even harsher criticism than that directed at the Region.

¹ PHIPA Order HO-007.

² as required by Section 12(1) of the *Personal Health Information Protection Act, 2004* (“PHIPA”) S.O. 2004, c.3, Schedule A.

³ as required by Section 12(1) of PHIPA

⁴ as required by Section 13(1) of PHIPA.

⁵ Order HO-004 at 19.

⁶ see for example: Order HO-005 involving the need to encrypt video surveillance systems, issued June 7, 2007; Fact Sheet No. 12: Encrypting Personal Health Information on Mobile Devices, issued May 2007; and various presentations and speeches, all available on the IPC’s website.

⁷ as required by Section 13(1) of PHIPA.

⁸ In particular, PHI was collected to determine whether individuals attending clinics were members of priority groups, even after the vaccine was made available widely to everyone in the Province, and health card numbers were collected even though other identifying information collected was sufficient. This was contrary to the obligation to limit collection of PHI to that which is necessary to fulfill identified purposes, as required by Section 30(2) of PHIPA.

⁹ The IPC found that the HIC had failed to take reasonable steps to ensure that PHI was secured against theft, loss and unauthorized use or disclosure, as required by Section 12(1) of PHIPA.

¹⁰ as required by Section 15(3) of PHIPA.

¹¹ Which it was required to do by Section 12(2) of PHIPA.

¹² The IPC found that an employee’s lack of training resulted in the HIC’s failure to comply with section 15(3)(b) of PHIPA (the requirement to ensure that all agents



GARDINER ROBERTS

were informed of their duties) despite his best efforts. The IPC noted: *I recognize that not all public health units may provide a sufficient level of training for their staff on the requirements of the Act. Given that these staff deal with personal health information on a daily basis, such training is critical.*