PHIPA Order
HO-008

June 30, 2010

Information & Privacy Commissioner,
Ontario, Canada

Ann Cavoukian, Ph.D.
Commissioner

**Information and Privacy Commissioner,
Ontario, Canada**

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

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

Table of Contents

1.0 BACKGROUND

1.1 THE INCIDENT

On May 18, 2010, University Health Network's (UHN's) Vice President and Chief Information Officer notified the Office of the Information and Privacy Commissioner/Ontario (the IPC) that a nurse working for UHN had her laptop stolen from her car. UHN is one of Canada's largest teaching hospitals and is comprised of three hospitals: Toronto General Hospital, Toronto Western Hospital and Princess Margaret Hospital, all located in downtown Toronto.

The laptop that was stolen contained records of approximately 20,000 patients dating back to 2004. UHN initially believed that the laptop was encrypted, as required by its customary procedures. When a mobile device is reported lost or stolen, the practice of UHN's privacy office is to contact the Information Management (IM) department to verify the encryption status of the device. In this instance, it was determined that the laptop was not, in fact, encrypted, despite UHN's stated policy.

Information contained on the laptop included incident reports, operating room lists, research data sets and class lists for patient education sessions. Contained within this information were patient names, patient medical records numbers, types and dates of surgeries performed and physician information. The information on the laptop did not include health card numbers or patient addresses.

Upon learning of the incident, my office immediately opened a file to conduct a review of this matter under the Personal Health Information Protection Act (the *Act*).

1.2 IPC PRECEDENTS

Prior to discussing the details of this incident and the resulting investigation, it will be instructive to review past precedents of my office, which are painfully similar in nature. These past precedents pertain to the vulnerability of storing personal health information on mobile devices.

ORDER HO-004

In March of 2007, I issued Order HO-004 against The Hospital for Sick Children (SickKids.) The incident which resulted in the Order was exceedingly similar in nature as it involved records of personal health information that were contained on an unencrypted laptop computer which was also stolen from a vehicle. The laptop contained the personal health information of approximately 3,000 current and former patients of SickKids. Order HO-004 created the encryption standard required for all health information custodians when storing personal health information on mobile devices. Although this Order was directed at SickKids, it applied to all health information custodians who were expected to follow its provisions to protect personal health information within their organizations.

ORDER HO-007

In January of this year, 2010, I issued another Order on this subject, Order HO-007 involving the Medical Officer of Health for the Regional Municipality of Durham. This followed an investigation into a lost, unencrypted USB key containing the personal health information of nearly 84,000 people who had attended H1N1 immunization clinics in Durham Region.

Following our review, and of particular significance to this case, I ordered the Medical Officer of Health to:

- Immediately implement procedures to ensure that records of personal health information are safeguarded at all times, as required by sections 12(1) and 13(1) of the *Act*, specifically by ensuring that any personal health information stored on any mobile devices (e.g. laptops, memory sticks), is strongly encrypted; and

- Revise its written information practices in order to comply with and incorporate the requirements of the *Act* and its regulations, specifically to ensure compliance with the Order provision set out above, and to consult with my office prior to finalizing those information practices.

Consistent with Order HO-004, Order HO-007 clearly set out my expectations for all health information custodians in Ontario to ensure that records of personal health information stored on mobile devices are protected by strong encryption. The options were made clear – sever all personal identifiers or encrypt the data stored on mobile devices – Full Stop.

As this issue is of great significance to my office, I had issued a press release in which I re-iterated the following message:

> 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. 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.

2.0 CONDUCT OF THE INVESTIGATION:

Following notification by the Vice President and Chief Information Officer, I initiated a review and assigned the file to an Investigator, who immediately began to gather further information, including copies of relevant policies and procedures. Additional information was provided to my staff at a meeting on May 19, 2010, and in a written submission dated June 3, 2010.

The May 19, 2010, meeting was attended by staff from UHN, including the Vice President and Chief Information Officer, the Corporate Privacy Officer and an Information Security Officer. The following details were provided about the incident:

- On May 5th, the nurse involved in this matter was provided with a new laptop from the hospital's IM department.

- In accordance with UHN's customary procedures, when a new laptop is initially connected to the UHN server, the start-up process includes an encryption package which is automatically launched. Encrypted devices are equipped to send status updates to the server, which retains a log of each event. In this case, at some point during the start-up, the encryption software did not properly engage and load onto the laptop. When this occurs, an error message is recorded on the server log and an error message stating, "Disk is not encrypted. Please encrypt this disk" appears on the laptop screen.

- When this message is displayed on the laptop, the IM staff member should recognize that the encryption process has failed, and as a result, must reinitiate the start-up process.

- An error message had indeed been recorded on the server log; however, staff in the IM department did not take note of it.

- Given that the server log received an error message, there was no reason to believe that an error message had not appeared on the laptop.

- The nurse involved reported to UHN that she could not recall if she had seen this message on the laptop screen.

- In accordance with UHN's customary procedures for issuing a new laptop, all information from the user's previous laptop is transferred over to the new laptop. In this particular case, this process included the transfer of all incident reports, operating room lists, research data sets, and class lists for patient education sessions.

- On May 7th, the nurse took the new laptop home in order to work on a document with a colleague on Saturday, May 8th. The nurse reported that she worked on the document until 4 p.m. on May 8th, and placed the laptop back in her car around 4:30 p.m. On Monday morning at 7:30 a.m., the nurse noticed that the laptop was no longer in the front seat of her car. The nurse was unable to recall if the laptop was on the front seat from the time she had placed it there on Saturday afternoon, to the time she noticed it missing on Monday morning, making it impossible to pinpoint the exact time when the laptop went missing.

- UHN advised that there was no sign of forced entry and the nurse was unable to recall whether her car had been locked.

- The nurse then reported the missing laptop to the police as well as to UHN Security, the IM department, her Clinical Director and the Risk Management/Privacy Office.
- UHN was able to confirm the extent of the information stored on the nurse's new laptop by checking her old device.

3.0 ISSUES ARISING FROM THE INVESTIGATION:

I identified the following issues, which will be discussed in turn, as arising from this review:

(A) Is UHN a "health information custodian" as defined in section 3(1) of the *Act* and were the nurse and IM staff member acting as "agents" of the health information custodian pursuant to section 2 of the *Act*?

(B) Are the records at issue "records" of "personal health information" as defined in sections 2 and 4 of the *Act*?

(C) Did the Health Information Custodian have information practices that comply with the requirements of the *Act* and did the Health Information Custodian comply with these practices as required by sections 10(1) and (2) of the *Act*?

(D) Did the Health Information Custodian comply with section 13(1) of the *Act* by ensuring that records of personal health information were retained and transferred in a secure manner?

(E) Did the Health Information Custodian comply with section 12(1) of the *Act* by taking reasonable steps to ensure that personal health information was secured against theft, loss and unauthorized use or disclosure and was notice provided in accordance with section 12(2) of the *Act*?

(F) Did the Health Information Custodian ensure that all agents were informed of their duties as required by section 15(3)(b) of the *Act*?

4.0 RESULTS OF THE INVESTIGATION:

Issue A: Is UHN a "health information custodian" as defined in section 3(1) of the *Act* and were the nurse and Information Management staff member acting as "agents" of the health information custodian pursuant to section 2 of the *Act*?

Section 3(1) of the *Act* states, in part:

> "health information custodian", subject to subsections (3) to (11), means a person or organization described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph, if any:
>
> 4. A person who operates one of the following facilities, programs or services:
>
> i. A hospital within the meaning of the *Public Hospitals Act*…

UHN is considered a "person" who operates a hospital within the meaning of the *Public Hospitals Act*. I am satisfied that UHN is a health information custodian as defined in section 3(1)4(i) of the *Act*. UHN agrees with this finding.

With regard to whether the nurse and the IM staff member who provided her with the new laptop are "agents" of UHN (the Custodian), section 2 of the *Act* defines an agent as follows:

> "agent," in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated;

In addition, section 17(1) of the *Act* states:

> A health information custodian is responsible for personal health information in the custody or control of the health information custodian and may permit the custodian's agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if,
>
> (a) the custodian is permitted or required to collect, use, disclose, retain or dispose of the information, as the case may be;
>
> (b) the collection, use, disclosure, retention or disposition of the information, as the case may be, is in the course of the agent's duties and not contrary to the limits imposed by the custodian, this Act or another law; and
>
> (c) the prescribed requirements, if any, are met.

Both the nurse and the IM staff member are employed by, and are authorized to act on behalf of, the Custodian in respect of personal health information. As such, I find that both the nurse and the IM staff member are "agents" of the Custodian as defined in section 2 of the *Act*. The Custodian does not dispute this finding.

As a result, UHN, as the Custodian, is responsible for all personal health information collected, used, disclosed, retained or disposed of by these agents on its behalf pursuant to section 17(1) of the *Act*.

Issue B: Are the records at issue "records" of "personal health information" as defined in sections 2 and 4 of the *Act*?

Section 2 of the *Act* defines a record as:

> …a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record.

Section 4(1) of the *Act* states, in part:

In this *Act*,

> "personal health information", subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information,
>
> (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, or
>
> (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,

Section 4(2) of the *Act* states:

> "identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

The information contained on the missing laptop included patient names, patient medical record numbers, types and dates of surgeries and the names of physicians who provided health care to these patients. Based on this information, I am satisfied that the records at issue are records of personal health information as defined in sections 2 and 4 of the *Act*. The Custodian agrees with this finding.

Issue C: Did the Health Information Custodian, comply with sections 10(1) and (2) of the *Act*?

Section 10(1) of the *Act* provides as follows:

> A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations.

Section 10(2) of the *Act* states:

> A health information custodian shall comply with its information practices.

During the course of this investigation, a number of the Custodian's policies were reviewed by my office, including:

- Storage, Transport & Destruction of Confidential Information
- Appropriate Use of Technology
- Computer Workstations
- Incident Reporting & Review
- Privacy
- Clinical Research Training
- Investigation & Reporting of Suspected Theft

In addition to the above policies, the Custodian provided a synopsis of its process for deploying encryption on mobile devices, including when new laptops are provided to staff members. The Custodian advised that the encryption software is expected to deploy automatically, along with other enhancements, when a newly issued laptop is initially connected to their network. This process takes 2 to 4 hours depending on the size of the hard drive. Once the encryption software is installed, a message is sent back to the central server indicating that the process has been completed.

As discussed earlier, this process was followed in the particular case under review. With the failure of the encryption software to properly deploy, an error message would have been displayed on the laptop's screen, as well as being sent back to the central server to indicate that there was a malfunction. We were advised that such an error message had been sent back to the server, indicating the failure of the encryption software to engage. Unfortunately, no action was taken by the IM department to respond to this error message and the nurse could not recall seeing the error message on the laptop screen. Further, the Custodian does not have a policy that requires the IM department to monitor and respond to error messages on the central server. Nor did it appear to be a practice that was engaged in by the IM staff.

The laptop went missing over the course of a weekend, and within days of being issued to the nurse. Once the loss was discovered, the privacy office contacted the IM department to verify the encryption status of the device. When the IM department checked the central server, it determined that the laptop was not, in fact, encrypted. As a result, the Custodian undertook a review of all laptops issued to staff. This review found that, in another 14 instances, the encryption package had failed to properly install, rendering all personal health information stored on those laptops vulnerable to loss, theft or unauthorized use and disclosure.

A number of the policies provided by the Custodian as part of this investigation are relevant to the circumstances of this incident. These policies need to be examined in the context of this specific fact situation in order to determine whether they comply with the requirements of the *Act*.

The Custodian's *Storage, Transport & Destruction of Confidential Information* policy clearly states:

> Removal of PHI or corporate information from UHN premises is prohibited except in transit between UHN locations and/or when necessary for the provision of health care. When in transit, PHI or other confidential information must be securely stored and in the custody and control of the individual at all times.

In addition, the policy goes on to state:

> PHI or corporate confidential, electronic information must be stored on the secure UHN Network, where possible. Where PHI must be stored on the local drive for patient care purposes, it must be de-identified, where possible.

In August of 2008, the Custodian updated its *Appropriate Use of Technology* policy. This policy makes specific reference to the user's obligation to securely protect personal health information:

> Users must make reasonable efforts to protect personal health information (PHI) and corporate confidential information in electronic form. Such efforts include, but are not limited to:
>
> - Storing information on a UHN secure network. Where PHI and corporate confidential information must be stored on the local drive for patient care purposes they must be de-identified or encrypted, where possible. Tools or software requiring hard drive storage for patient care functions must be reported to the UHN Privacy Office.
>
> - De-identifying PHI and corporate confidential information where possible.

Regarding portable devices the policy goes on to state:

> Portable (mobile) devices must be secured at all times. A cable lock with an audible alarm may be used while working with the portable device, or the portable device may be locked away when not in use. When in transit, the user must ensure that the portable device remains in his/her possession at all times.
>
> PHI and corporate confidential information must not be carried on the portable device unless absolutely necessary. If carrying such information is necessary, it must be de-identified, where possible.
>
> When no longer needed, all PHI and corporate confidential information must be removed from portable devices.

Finally, in its *Computer Workstations* policy, the Custodian reiterates to staff the importance of storing personal health information on the hospital server or, if necessary on an encrypted drive. The *Computer Workstations* policy applies to "all workstations managed by Hospital IT that provide business services, including, but not limited to, laptops, tablet PCs, desktops, thin clients and personal digital assistants (PDAs)." This policy provides the following direction:

- Store all business-critical and confidential patient or corporate data on Hospital IT servers, wherever possible, to prevent data loss and/or data compromise and to ensure backup of the data. Where personal health information must be stored on the local drive for patient care purposes, the drive must be encrypted and, where possible, the information must be de-identified.

- Have all mobile computers (notebooks, tablets, etc.) managed by Hospital IT and these must be encrypted using standard full-disk encryption software as defined by the information security officer. Other workstations may be encrypted as deemed necessary by the privacy and/or information security officer.

Before beginning an analysis of these policies in relation to this case, it is crucial that I speak to the phrase "where possible" when referring to either the de-identification of information or the encryption of it. This phrase consistently appears in each of these policies and may cause some confusion by suggesting that it may be permissible, in some circumstances, to have personal health information on a mobile device that is both unencrypted **and** identifiable — this is not the case. Personal health information **must** either be de-identified or encrypted. Even with encryption, custodians have an obligation to only use identifiable personal health information if other information will not serve the purpose and to only use the minimum necessary to serve the purpose. Thus, even if custodians have encryption in place, they should only use de-identified data if its use will serve the purpose involved. If neither de-identification nor encryption is "possible," then **no** personal health information may leave the custodian's premises. I will address this in my Order provisions.

In this case, the facts indicate that the personal health information was not securely stored, nor was the laptop in the custody or control of the nurse at all times. Despite having various policies which outline the obligations of staff to protect personal health information in transit, the nurse, by removing the laptop from the Custodian's premises and leaving it unattended on the front seat of her car over the course of the weekend, was clearly not in compliance.

Further exacerbating the situation, the Custodian acknowledged that it was not even necessary for the nurse to have the records of personal health information on the laptop. This contravened the *Storage, Transport and Destruction of Confidential Information* policy which prohibits the removal of personal health information from the Custodian's premises except in transit, between locations, and when necessary for the provision of health care. In fact, the records were for the most part, historical in nature and not an adjunct to the nurse's duties and activities. According to the Custodian, the records were placed on the new laptop as a matter of routine. The practice of the IM department when issuing new laptops to staff members was to simply transfer any information stored on the old laptop to the new device. No process was in place to review records stored on old machines to ensure that only necessary records were retained on the new laptop,

and unnecessary records deleted. The Custodian advised in its written submission that the nurse was not aware of the actual amount of personal health information stored on her laptop.

To reiterate, the Custodian acknowledges a number of instances where the nurse had not complied with established information practices. The laptop was left unattended on the front seat of the nurse's car and was not in her possession at all times, as required by the *Appropriate Use of Technology* policy. The personal health information contained on the laptop was not de-identified, a further contravention of the *Appropriate Use of Technology* policy. In fact, the personal health information should never have been transferred from the nurse's old laptop to the new device. I will address this in my Order provisions.

The facts also indicate, and the Custodian agrees, that there was a critical failure to ensure that the records of personal health information stored on the laptop were encrypted. The *Computer Workstations* policy clearly states that the responsibility for managing workstations, including mobile devices, rests with the IM department. In this incident, the IM staff member delivered the laptop and launched the deployment of the software at the nurse's workstation. However, the IM staff member did not verify that the entire process had been successfully completed, including the loading of the encryption function. The Custodian advised that while there were processes in place to encrypt the devices, there were no practices or requirements in place to verify the encryption status of these devices.

The Custodian has since changed its practice in light of this incident to ensure that the IM staff uploads all software *prior* to providing staff members with any mobile device. IM staff will not only upload all required packages but will verify the completion of the upload to ensure that all software is working properly, and that the encryption package has been successfully engaged. Had this information practice been in place prior to May of 2010, the theft of this laptop would have been much less serious.

Finally, the Custodian reported that once the encryption software had failed to properly upload onto a new laptop, an error message would have been displayed once the nurse had turned on the device. In addition, a similar error message would have been sent to the central server (which we know was indeed sent). In this case, there is no evidence that such an error message was acted upon by either the nurse or an IM staff member. In addition, as mentioned earlier, this was not an isolated incident. According to the Custodian, encryption software failed to properly deploy on laptops in 14 other instances. It is clear that any error messages sent to the IM department on those occasions were also not monitored or responded to and all personal health information on those laptops remained unencrypted.

The Custodian has invested a great deal of time and energy in developing information practices that are compliant with the requirements of the *Act*. However, based on the facts of this case and a careful review of the relevant information practices, I consider these practices to be deficient.

I note that the information practices relating to the secure retention of records of personal health information on mobile devices, including laptops, may be found in various policies and procedures, which could potentially result in confusion for staff seeking guidance in this regard. It is also apparent that the Custodian places great reliance on mobile devices to enable

the delivery of health care to its patients. While I fully accept the value of such devices, the risk of theft or loss from the use of mobile devices is so high, and the consequences potentially so serious, that a health information custodian placing such reliance on them should develop a "stand-alone," comprehensive policy for mobile devices setting out, in one location, the clear expectations and requirements for staff, both clinical and IM.

I recognize that the scope of the *Computer Workstation* policy goes beyond desktop computers and includes laptops and PDA's. However, a comprehensive mobile device policy should be broader, for example, by covering USB sticks and portable disks. I am also not satisfied that a staff member looking for the Custodian's policy on the use of laptops or PDA's would be drawn to the *Computer Workstation* policy. A policy dedicated to mobile devices would have the advantage of clarity and simplicity by setting out the rules for all staff in one location, rather than requiring staff to review multiple policies.

The facts of this case demonstrate other deficiencies in the existing policies, primarily by not considering the particular circumstances involved in issuing new laptops, or other mobile devices, to staff. Specifically, the existing information practices failed to:

- Require the IM department to ensure that encryption software was fully functional prior to issuing a mobile device to staff members;
- Require staff members to use the receipt of a new mobile device as an opportunity to review any records of personal health information stored on the old device and purge those records no longer required; and
- Ensure that the IM department monitors and responds immediately to any error messages indicating that encryption software has malfunctioned.

As a result, I find that the Custodian did not have in place adequate information practices that comply with the requirements of the *Act*; therefore the Custodian did not comply with section 10(1) of the *Act*.

Similarly, I am satisfied that the nurse and IM staff member, as agents of the Custodian, did not comply with the information practices in place at the time of the incident. Specifically, the IM staff member failed to ensure that the records of personal health information on the nurse's laptop were encrypted. The nurse unnecessarily removed records of personal health information from the hospital premises. Further, she did not securely store the laptop containing the records of personal health information and did not retain the laptop in her custody and control at all times. As a result, I find that the Custodian did not comply with section 10(2) of the *Act*.

I would like to acknowledge that as a result of this incident, the Custodian has taken a considerable number of steps to reduce the likelihood of a re-occurrence. These involve clarifying roles and responsibilities when issuing new mobile devices, as well as placing greater emphasis on the need to regularly "clean-up" workstations, laptops and other electronic devices by removing unneeded records of personal health information. However, for greater clarity and certainty, I will address the Custodian's non-compliance with sections 10(1) and (2) in my Order provisions.

Issue D: Did the Health Information Custodian comply with section 13(1) of the *Act*?

Section 13(1) of the *Act* provides as follows:

> A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any.

It is not disputed by the Custodian that large numbers of records of personal health information were retained on an unencrypted laptop which was subsequently stolen from a staff member's car. As discussed under Issue C, I have already found that the Custodian's information practices at the time of this incident were inadequate, and that agents of the Custodian did not comply with those information practices that were in place. Similarly, I also find that the Custodian did not ensure that the records of personal health information in its custody or under its control were transferred in a secure manner and, therefore, they did not comply with section 13(1) of the *Act*. The Custodian does not dispute this finding.

The failure of the Custodian to comply with section 13(1) will be addressed by the Order provisions made in conjunction with Issue C.

Issue E: Did the Health Information Custodian comply with section 12(1) and (2) of the *Act*?

Section 12(1) of the *Act* provides as follows:

> A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

Section 12(2) of the *Act* provides as follows:

> Subject to subsection (3), and subject to the exceptions and additional requirements, if any, that are prescribed, a health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost or accessed by unauthorized persons.

In light of the facts of this case and my findings of non-compliance under Issues C and D, I find that the Custodian did not take steps that were reasonable in the circumstances to ensure that personal health information in its custody or control was protected against theft, loss and unauthorized disclosure and to ensure that the records of personal health information were protected against unauthorized copying, modification or disposal as required by section 12(1) of the *Act*. The Custodian therefore has an obligation pursuant to section 12(2) to notify affected individuals about the loss of their personal health information.

The Custodian has advised my office that, where contact information for a patient appeared to be current, affected individuals were sent a letter to advise them of this incident. In total, the Custodian has sent out 705 letters.

Where contact information appeared to be out of date, the Custodian placed an electronic flag on the file for each affected individual and individual letters were added to the related patient charts. This step was taken for 19,337 individuals. Should those patients return for treatment, they will be advised to contact the Privacy Office, who in turn will advise them of the incident and provide them with their written notice.

In addition, the Custodian issued a News Release on May 28, 2010, which has also been posted to their website, to advise the public of this breach. The Custodian also established a dedicated telephone line to answer any questions or concerns the public may have regarding this incident.

Based on all of the above actions taken, I find that the Custodian has complied with section 12(2) of the *Act*.

Issue F: Did the Health Information Custodian comply with section 15(3)(b) of the *Act*?

Section 15(1) of the *Act* provides as follows:

> A health information custodian that is a natural person may designate a contact person described in subsection (3).

Section 15(3) of the *Act* provides as follows:

> A contact person is an agent of the health information custodian and is authorized on behalf of the custodian to,
>
> (b) ensure that all agents of the custodian are appropriately informed of their duties under this *Act*;

The Custodian has appointed a Corporate Privacy Officer to, among other things, ensure that all agents of the Custodian are appropriately informed of their duties under the *Act* as required under section 15(3)(b).

The Custodian advised that, prior to this incident, they had undertaken a number of communication strategies to ensure that staff were aware of their obligations to protect personal health information in accordance with the *Act*. The Custodian provided my office with a number of communications initiatives that dealt specifically with privacy matters, including:

- Past issues of *Straight Talk* – a regular communication tool for UHN's CEO to communicate with staff;
- *UHN News* – the weekly staff publication for UHN staff across the sites; and

- U*HN Risk Management newsletter* – sent out to advise staff of risk management/ privacy related matters.

In addition, the Custodian provided samples of their *Privacy in Practice* series – an excellent initiative – which was created in partnership with another downtown Toronto hospital. Since the beginning of June 2009, the series has appeared throughout the Custodian's facilities and includes posters, information packages, digital messages on television screens across the sites, intranet postings and training sessions for all staff, medical students, residents and fellows. The Custodian also advised in its written submissions that the following sessions include privacy-related training:

- New Employee Orientation program – mandatory for all new personnel;
- Volunteer Orientation – mandatory for all new volunteers;
- Physician eLearning module – mandatory completion by all MDs in 2010; and
- Various In-services.

The Custodian's President and CEO, Dr. Bob Bell, released a notice to all staff to address this incident in his regular series, *Straight Talk*. In addition to advising staff of the incident, he reminded them of their responsibility for ensuring that computers and laptops with patient information be protected from theft or fraud. He further reminded staff that laptops and computers are to be securely stored at all times, patient information is to be saved on the secure network, not on desktops, and staff are to double check that any mobile devices provided by the IM department have been encrypted. In addition, the Custodian will be targeting staff with reminders of their obligations under the Act through Medical Staff Bulletins, Lunch 'n' Learns, as well as through continuing education sessions which are already scheduled throughout the year.

While we acknowledge that the Custodian has provided extensive privacy training and awareness to staff, the facts of this incident indicate a deficiency in raising awareness of the particular issues surrounding the use of mobile devices. As noted in Issue C, hospitals such as this one, place great reliance on mobile devices in order to provide health services to patients. We acknowledge that mobile devices may be crucial to the successful delivery of such services, but they also pose a potential danger – they appear to be easily lost or misplaced, and present a tempting target for thieves. Although the nurse and IM staff member involved in this incident had been exposed to privacy and security training, the Custodian has confirmed that training is not provided to its employees that is specifically dedicated to mobile devices. This is just the latest in a series of incidents involving health information custodians that demonstrates why such training is critical. Staff members must continually be reminded of their responsibilities when dealing with mobile devices, and this training may vary depending on the staff involved. For example, clinical staff will have different responsibilities than staff in the IT department. In my view, comprehensive, ongoing, role-based privacy and security training regarding the issues related to mobile devices, may have prevented this incident from occurring.

Given the importance of mobile devices to the operations of the Custodian, it is important that all agents using mobile devices issued by the Custodian, or who are involved in the issuance of such devices, receive specific training. Consequently, I must find that the Custodian did not comply with section 15(3)(b) of the *Act* by ensuring that all of its agents are appropriately informed of their duties under the *Act*. I will address this omission in my Order provisions.

5.0 SUMMARY OF FINDINGS:

I have made the following findings in this review:

1. University Health Network is the "health information custodian" as defined in section 3(1) of the *Act* and the nurse and IM staff member were acting as "agents" of the Custodian pursuant to section 2 of the *Act*.

2. The records at issue are "records" of "personal health information" as defined in sections 2 and 4 of the *Act*.

3. The Custodian did not comply with sections 10(1) of the *Act* nor did the Custodian comply with section 10(2) of the *Act* as it did not have in place information practices that comply with the requirements of this *Act* and it did not comply with its information practices.

4. The Custodian did not comply with section 13(1) of the *Act* as it did not ensure that the records of personal health information in its custody or under its control were retained, transferred and disposed of in a secure manner.

5. The Custodian did not comply with section 12(1) of the *Act* as it did not take steps that were reasonable in the circumstances to ensure that personal health information in his custody and control was protected against theft, loss and unauthorized use or disclosure. The Custodian did comply with section 12(2) of the *Act* by fulfilling its obligation to notify affected individuals.

6. The Custodian did not comply with section 15(3)(b) of the *Act* as it did not ensure that all agents of the Custodian are appropriately informed of their duties under this *Act*.

6.0 ORDER:

I order the Custodian to immediately develop and implement practices and procedures to ensure that records of personal health information stored on mobile devices are safeguarded at all times as required by sections 12(1) and 13(1) of the *Act*. Specifically, I order the Custodian to:

1. Develop and implement a comprehensive corporate policy and accompanying procedures relating to the secure retention of records of personal health information on all mobile devices (e.g. laptops, memory sticks, PDA's). At a minimum, the policy and its procedures must include the following elements to specifically address this incident:

a. Any personal health information stored on any mobile device is to be strongly encrypted.

b. The Information Management Department is to be charged with the responsibility of ensuring that encryption software on mobile devices is properly deployed and in working order before issuing the devices to staff.

c. The Information Management Department, specifically the Chief Information Officer, is to be charged with the responsibility of receiving immediate notice of any encryption errors messages which are received by the main server. Upon receipt of error messages of this type, ensuring that the Chief Information Officer is responsible for the immediate investigation and correction of such errors.

d. Guidelines for use by staff when receiving new mobile devices. These guidelines must require staff to review and purge all personal information, including personal health information, to be transferred onto the new mobile device, to ensure that only information required for performance of their duties is retained and placed on the new device. In addition, a copy of these guidelines must be provided by the IM department to staff when a new mobile device is issued in order to serve as a reminder to purge old information which is no longer necessary.

2. Conduct a review of all UHN policies to ensure that clear direction is provided when records of personal health information are being removed from its premises on mobile devices. Specifically, policies must state that records of personal health information on mobile devices are to either be de-identified or strongly encrypted. Under no circumstances should records of personal health information on mobile devices be identifiable and unencrypted.

3. Enhance education and awareness programs: Develop and implement comprehensive, ongoing, role-based privacy and security training pertaining to the risks posed by the deployment and use of mobile devices.

In order to verify compliance with this Order, I require that the Custodian provide me with proof of compliance by September 30, 2010.

7.0 RECOMMENDATIONS:

1. In order to ensure that a practice is established to proactively check for error messages indicating that encryption software has not properly loaded onto a mobile device, I recommend that, for the next six months, the President and CEO of UHN, review the encryption error message alerts and sign-off on any follow-up undertaken by the Chief Information Officer and the Information Management Department, in order to ensure compliance with this Order.

2. To ensure that all staff at the Custodian's facilities are familiar with the requirements set out in the Order provisions above, I recommend that the President and CEO of UHN send a message through his regular staff communication (*Straight Talk*) advising staff of this Order and convey to staff the seriousness of this breach, the specific policy and procedural changes resulting from this Order and the importance of continued diligence in protecting personal health information, in accordance with the *Act*.

June 30, 2010

Ann Cavoukian, Ph.D.
Commissioner

Date

Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada
416-326-3333 1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca
Email: info@ipc.on.ca