Encrypt Your Mobile Devices:
Do It *Now*

PHIPA Order
HO-007

January 14, 2010

Information & Privacy Commissioner,
Ontario, Canada

Ann Cavoukian, Ph.D.
Commissioner

Information and Privacy Commissioner/Ontario

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
Website: www.ipc.on.ca

Table of Contents

1.0 EXECUTIVE SUMMARY

Three years ago, in 2007, following the loss of a laptop computer containing personal health information, the Information and Privacy Commissioner of Ontario (IPC) sent a clear message to all health information custodians against storing unencrypted personal health information on mobile devices. Order HO-004 outlined a new standard to be followed to protect personal health information on mobile devices and created the expectation that all custodians would comply with this requirement. The fact that three years later, health care providers would be unaware of this requirement is both disappointing and unacceptable.

On December 21, 2009, the IPC was notified by the Regional Municipality of Durham's Medical Officer of Health, Dr. Robert Kyle, that a public health nurse working for the Durham Health Department had lost a USB memory stick containing the personal health information of 83,524 individuals who had attended H1N1 immunization clinics in Durham Region. This information was collected from these individuals when receiving the H1N1 vaccine at one of eight community clinics. The personal information included their names, addresses, telephone numbers, dates of birth, health card numbers and additional health information regarding their health history. Most important and truly regrettable — the memory stick was not encrypted, despite the fact that the encryption of mobile devices was required as of Order HO-004 in 2007.

My Office immediately initiated an investigation into this serious breach of the *Personal Health Information Protection Act* (*PHIPA*). In addition to conducting interviews with the appropriate staff of the Durham Health Department and the Regional Municipality of Durham, I contacted the province's Chief Medical Officer of Health, Dr. Arlene King, as I was concerned that other public health units might be conducting H1N1 immunization clinics without the proper safeguards in place to protect the personal health information of Ontarians. On December 24, 2009, Dr. King issued a memorandum to all medical officers of health in Ontario urging them to immediately cease storing or transferring personal health information on mobile devices unless they had strong encryption in place.

In addition, to alleviate any concern regarding ongoing immunization clinics in Durham Region, my staff provided Regional information technology staff with a ready-to-deploy encryption software solution offered by CryptoMill, an Ontario-based company.

My investigation determined that memory sticks were used by the Durham Health Department as a temporary measure to transfer personal health information between the eight community clinics and Regional Headquarters. However, due to problems in establishing a Virtual Private Network, the memory sticks became a permanent means to transfer the information. Unfortunately, the Durham Region staff person providing technical support to the clinics was unaware of the requirement to encrypt the memory sticks and had never received *PHIPA* training. As a result, unlike the seasonal flu clinics operated by the Durham Health Department, the personal health information of H1N1 vaccine recipients remained unprotected by appropriate safeguards. This represented a serious breach of the Medical Officer of Health's responsibilities under *PHIPA*, and was completely avoidable.

My investigation also concluded that the Durham Health Department breached *PHIPA* by collecting more personal health information from H1N1 vaccine recipients than was necessary for the purposes of the immunization clinics. Specifically, a convincing rationale was not provided for the collection of health card numbers or information relating to priority group status after the H1N1 vaccine was made widely available to the general public.

Based on the findings of this investigation, I ordered the Medical Officer of Health for Durham Region to take a number of actions, including:

- Immediately implementing procedures to ensure that records of personal health information are safeguarded at all times, specifically by ensuring that such records stored on mobile devices are strongly encrypted;

- Revising the written information practices of the Durham Health Department to comply with the requirements of *PHIPA*, particularly the need to strongly encrypt personal health information on mobile devices;

- Ceasing the collection of the health card numbers of individuals attending H1N1 immunization clinics as well as personal health information pertaining to priority group status; and

- Securely destroying the health card numbers collected from H1N1 immunization clinic attendees as well as any personal health information relating to priority status collected from individuals, after the H1N1 vaccine was made widely available to the general public.

My Order also included a recommendation directed to the Regional Municipality of Durham, an institution subject to the *Municipal Freedom of Information and Protection of Privacy Act*. In order to address deficiencies in the Region's information practices and to ensure that all personal information under its custody and control is protected, I have recommended that Durham Region develop and implement a comprehensive corporate policy for mobile devices to ensure that, to the extent that personal information must be transported on those devices, it is strongly encrypted.

The Order also recognizes the leadership role that the Ministry of Health and Long-Term Care plays in providing guidance to the 36 public health units in the province. As a result, I have recommended that the Ministry take the following actions, in conjunction with the province's Chief Medical Officer of Health:

- Request each public health unit to 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;

- Request that each medical officer of health in the province provide the Ministry with an attestation that no unencrypted personal health information is being transported on mobile devices;

- Audit a representative sample of public health units to verify the information provided by the medical officers of health; and

- Provide resources to the Chief Medical Officer of Health for the development of training materials to ensure that all public health unit staff are aware of the need for proper safeguards for personal health information stored on mobile devices.

Finally, in order to ensure that residents of Durham Region are made aware of the results of this investigation and the steps that have been taken to ensure that a similar incident does not happen again, I have recommended that the Durham Region Medical Officer of Health inform the public about the issuance of this Order and how to obtain a copy. I have asked that this include placing advertisements in local newspapers in the Durham Region, and directing the public to the IPC website to obtain a copy of the Order.

2.0 BACKGROUND

2.1 *The Incident*

On December 21, 2009, the Regional Municipality of Durham's Medical Officer of Health, Dr. Robert Kyle, notified the Office of the Information and Privacy Commissioner of Ontario (the IPC) that a public health nurse working for the Durham Regional Health Unit (Durham Health Department) had lost a USB memory stick containing the personal health information of 83,524 individuals who had attended H1N1 immunization clinics in the Durham region during the period of October 23, 2009 to December 15, 2009. As a result, and given the unprecedented size of this breach, the IPC immediately initiated an investigation and review pursuant to section 58 of the *Personal Health Information Protection Act* (the *Act*).

The Medical Officer of Health advised the IPC that on December 16, 2009, the nurse was on her way from Durham Regional Headquarters to an H1N1 immunization clinic and discovered that she had lost the memory stick as she walked from the main building to her car in the parking lot. Unable to find the memory stick, the nurse reported the loss to her management staff immediately and to the Corporate Information Services Department (CIS) the following morning.

Durham Health Department staff undertook a number of immediate steps to locate the missing memory stick. A search was conducted of the parking lot, the route the nurse had taken and the nurse's purse, car, clothing and workstation. They also viewed security tapes and interviewed staff members who may have had information regarding the loss of the memory stick. They also reported the loss to the Police. Unfortunately, despite these efforts, the missing memory stick could not be located.

The Medical Officer of Health advised the IPC that the memory stick contained a significant amount of personal health information relating to individuals who had received the flu shot, including their names, addresses, telephone numbers, genders and dates of birth; health card numbers and expiry dates; names of primary physicians of flu shot recipients; and additional personal health information provided by recipients regarding their health history (e.g. pregnancy, allergies, cardiac or pulmonary diseases, or diabetes).

In addition, user IDs, passwords and security levels of staff (i.e., administration staff, nurses, clinical leaders, IT staff, health staff) that had access to the Niagara Mass Immunization Data Collection System were also contained on the memory stick.

Most important and truly regrettable, the Medical Officer of Health also advised the IPC that the missing memory stick was not encrypted.

Following notification from the Medical Officer of Health that the missing memory stick was unencrypted, I was extremely concerned that public health units in other areas of Ontario may also be conducting immunization clinics with the use of unencrypted mobile devices, and as a result, threatening the privacy of flu shot recipients. My office immediately contacted Ontario's Chief Medical Officer of Health and arranged for a meeting on December 24, 2009. As a result

of that meeting, a memo was sent by the Chief Medical Officer of Health to all Medical Officers of Health in Ontario, urging them to immediately cease storing or transferring personal health information on mobile devices unless they have strong encryption in place.

In addition, I issued a news release, on December 24, 2009, available on the IPC's website, www.ipc.on.ca/images/Resources/2009-12-24-encrypt_phi.pdf, that directed the province's health sector not to remove any personal health information from their premises on mobile devices, unless it was encrypted, as required in my previous Order HO-004, issued in March of 2007.

As a result of the publicity brought to this issue, my office was contacted by many individuals who were anxious to have the circumstances of this breach investigated by my Office, and who expressed concern that the loss of their personal health information and that of their families could lead to identity theft. This increased my determination to proceed swiftly with this investigation and issue this Order as quickly as possible.

2.2 *IPC Precedent – Order HO-004*

Before discussing the details of this incident and the resulting investigation, it is critical to describe Order HO-004 in greater detail. The incident resulting in that Order was similar in nature as it involved records of personal health information that were contained on an unencrypted laptop computer. The laptop was stolen from a physician's vehicle, and contained the personal health information of approximately 3,000 patients of The Hospital for Sick Children (SickKids).

Following the review, I issued Order HO-004, which emphasized the obligations imposed on a health information custodian by the *Act* to ensure that records of personal health information in its custody or control are retained in a secure manner and that steps are taken to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure. In particular, I concluded:

> As a first line of defence against unauthorized access, custodians should avoid storing identifiable [personal health information] on mobile computing devices. However, where [personal health information] must be stored on such devices, only the minimal amount of information necessary should be stored, and for the minimal amount of time necessary to complete the work. In addition, where possible, [personal health information] should be de-identified or coded, in a manner such that the identities of the individuals whose [personal health information] is stored on the device could not be readily ascertained if the information were accessed by unauthorized persons.
>
> ***Where identifiable [personal health information] is stored on vulnerable devices, such as laptop computers or flash drives, my position is that the information must be encrypted.*** [emphasis added]

As a result, Order HO-004 contained extensive order provisions directed in particular to SickKids. Of direct relevance to this investigation, I ordered SickKids to:

- Develop or revise and implement policies and procedures to ensure that records of personal health information are safeguarded at all times pursuant to the *Act*;
- Ensure that its information practices comply with and incorporate the requirements of the *Act*, including a policy that personal health information that is removed from the hospital in electronic form must be either de-identified or encrypted;
- Develop and implement a hospital-wide endpoint electronic devices policy, applicable to both desktop and portable devices (e.g. laptops, PDAs), which mandates that any personal health information not stored on secure servers must either be de-identified or encrypted; and
- Provide education and training to staff members, researchers and clinicians on the risks associated with the use of laptop computers, as well as detailed instructions on how to secure the information contained on laptop computers and regarding its new policies, on a regular and recurring basis.

The *Act* requires custodians to 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 and disclosure. Order HO-004 clearly sets out my interpretation of what would be reasonable in the circumstances where personal health information is stored on mobile devices. Thus, compliance with the encryption standard set out in Order HO-004 should have been viewed as a requirement for *all* health information custodians in Ontario. When I issued Order HO-004 in 2007, I expected all health information custodians to review their policies and procedures to ensure that any personal health information that had to be stored on portable devices was at all times encrypted. The fact that three years later a similar incident occurred, jeopardizing the personal health information of a large number of Ontarians, causes me great concern and is, quite frankly, completely unacceptable.

2.3 *Public Health In Ontario*

Prior to outlining the results of my investigation, it is important to outline the relationships between the various organizations and individuals involved in the delivery of immunization clinics in Ontario.

Public Health Units and Boards of Health

There are 36 public health units in the province, including the Durham Health Department. Each public health unit is governed by a board of health, largely made up of elected representatives from the local municipal councils, in this case the Regional Municipality of Durham. The duties of a board of health are set out in the *Health Protection and Promotion Act (HPPA)*. In general, boards of health are required to provide health programs and services in certain areas, including

the control of infectious and reportable diseases, the provision of immunization services to children and adults, as well as programs of health promotion and protection.

Medical Officer of Health

The board of health is an autonomous corporation under the *HPPA*. The medical officer of health reports directly to the board of health on issues relating to public health concerns and public health programs and services. The medical officer of health is responsible for day-to-day management decisions, such as directing the overall provision of programs and services of the public health unit, recommending appropriate changes and reporting these findings regularly to the board of health. The employees of, and the persons whose services are engaged by a board of health, are subject to the direction of the medical officer of health if their duties relate to the delivery of public health services or programs.

Ministry of Health and Long-Term Care and Ministry of Health Promotion

The Ministry of Health and Long-Term Care is responsible for administering the health care system and providing services to the Ontario public through a variety of programs including community and public health and health promotion and disease prevention. The Ministry of Health and Long-Term Care has a Public Health Division, headed by an Assistant Deputy Minister, who reports to the Deputy Minister of the Ministry of Health and Long-Term Care. The public health model in Ontario involves shared authority at both the provincial and municipal levels and the Ministry of Health and Long-Term Care partially funds Ontario's public health units.

The Ministry of Health Promotion was created in June, 2005. Its goals are to promote and encourage Ontarians to make healthier choices at all ages and stages of life, to create healthy and supportive environments, lead the development of healthy public policy and assist with embedding behaviours that promote health. The Ministry of Health Promotion also has a Public Health Division.

It is important to note for the purposes of this investigation that local medical officers of health do not have a direct reporting relationship to either Ministry.

Chief Medical Officer of Health

The role of the Chief Medical Officer of Health is one of leadership within Ontario's public health system, whether during a health crisis or on an ongoing basis, to inform, protect and promote the public's health.

The Chief Medical Officer of Health is in charge of the Public Health Division of the Ministry of Health Promotion and, as such, reports to the Deputy Minster of the Ministry of Health Promotion. In addition, the Chief Medical Officer of Health reports to the Deputy Minister of the Ministry of Health and Long-Term Care.

Again, it is important to note that for the purposes of this investigation, local medical officers of health do not have a direct reporting relationship to the Chief Medical Officer of Health.

2.4 *Niagara Mass Immunization Data Collection System*

As part of the delivery of H1N1 flu vaccination, the Niagara Mass Immunization Data Collection System (Niagara System) was developed through the efforts of the Ministry of Health and Long-Term Care (Ministry) and the Niagara Health Unit. This system was then made available to other health units in Ontario, including the Durham Health Department, to support the delivery of the H1N1 vaccine. Unfortunately , the IPC was never consulted about the Niagara System when it was being developed or prior to its introduction and implementation by the health units.

In November of this year, my office received two queries with respect to the nature and scope of information being requested at two specific H1N1 immunization clinics (neither of which involved the Durham Health Department), and the manner in which this information was being collected.

My office engaged in extensive discussions with the two public health units involved, as well as the Ministry in order to review the scope of information being collected and to ensure consistency and transparency in the collection of personal health information. We were advised that the H1N1 immunization data collection process is a collaborative effort among the Ministry, public health units and vaccine delivery agents outside of health units (e.g. physicians).

The Niagara System is a stand-alone system that was developed for collecting personal health information in H1N1 immunization clinics. The system was designed to collect personal health information for a variety of purposes including the provision of health care to individuals, determining whether individuals were members of priority groups, creating immunization records, and following-up with individuals in case of an adverse event. The Ministry provided funding for public health units that opted to employ the Niagara System and received certain aggregate information generated by the system. My office was advised that, of the 36 public health units in Ontario, 30 of them were using the Niagara System. This included the Durham Health Department.

As a result of our discussions with the Ministry, both the scope and nature of the aggregate information being collected by the Ministry was reduced significantly. In a memorandum dated December 1, 2009, the Ministry advised all public health units that "effective Wednesday, December 2, 2009, health units are being asked to provide only the following aggregate information on a weekly basis to the ministry: number of doses administered, age and gender." The memorandum further advised that "if health units choose to continue to collect personal health information (PHI) at immunization clinics for their own purposes, health units should ensure that they are complying with *PHIPA*, including any relevant notice/consent requirements."

In response to the Ministry's memorandum, the two public health units involved in the initial discussions concluded that it was no longer necessary for them to collect priority group information. They also agreed that the collection of health card numbers was not necessary for administering the immunization program. Consequently, both public health units indicated that this personal health information would no longer be collected.

In addition, individuals attending H1N1 immunization clinics were being asked to provide their health cards and driver's licences to public health units, which were then "swiped" through a magnetic reader. Individuals were not advised of the nature of the information being collected from the health cards and driver's licences, the purposes for which this information was being collected and used, and, most importantly, that they could elect *not* to provide health cards and driver's licences and still be entitled to receive their immunization. For example, with respect to driver's licences, individuals were not advised that the only information being captured from the driver's licence was their name, mailing address, date of birth and gender and that the purpose for which this information was being collected was to create an immunization record and to be able to contact individuals in the case of adverse events. The actual driver's licence number was not being captured during the "swiping" process. As a result of our intervention, both public health units prepared and posted notices providing this information.

3.0 CONDUCT OF THE INVESTIGATION

Following notification by the Medical Officer of Health of the loss of the memory stick, I initiated a review and assigned the file to an Investigator, who immediately began to gather further information including obtaining copies of relevant policies and procedures. These included policies and procedures from the Durham Health Department, the Durham Corporate Information Services (CIS) and the Regional Municipality of Durham (Durham Region). Additional information was provided to my staff at a meeting on December 29, 2009, and in a written response submitted on behalf of the Medical Officer of Health and Durham Region through their solicitor on January 5, 2010, in response to the IPC's request for written submissions.

On December 29, 2009, staff from my office, including the Manager of Mediation, an Investigator and a Senior Policy and Technology Advisor, met with staff at Durham Regional Headquarters, including: the Regional Clerk, the Medical Officer of Health, the Director and Assistant Director for the Public Health Nursing and Nutrition Division, the Supervisor and Director for Health Administration, the Director for Technical Services in the CIS Department, the Clerk for Records, and the Solicitor for the Durham Region.

My staff were advised that the past practice for seasonal flu immunization clinics has always been to encrypt all laptops, computers, and memory sticks. Unlike the seasonal flu immunization clinics, the decision was made to use the Niagara System to facilitate data collection for the H1N1 immunization clinics. At the time, it was believed by the Durham Health Department, that CIS (the unit of Durham Region providing technical support to the Durham Health Department) would have ensured that the Niagara System contained the same protections as the system used for the seasonal flu clinics. As such, when the nurse left Durham Regional Headquarters on December 16, 2009, heading to an immunization clinic, she believed she was transporting personal health information on an encrypted memory stick.

It was only after she reported the missing memory stick to CIS that she was advised the memory stick was *not*, in fact, encrypted. In addition, CIS learned that memory sticks for all eight immunization clinics distributed to staff as part of the Niagara System roll-out were unencrypted. As a result, all memory sticks that had been issued were recalled and all personal health information was deleted.

Further investigation revealed that when the CIS employee created the process for the use of the Niagara System, he did so without including the encryption of the memory sticks, as he had not been informed that encryption was a requirement.

My staff were advised that originally, a Virtual Private Network (VPN) was to be used as the method for securely encrypting and transferring personal health information to and from the community H1N1 immunization clinics and the main server at Regional Headquarters. The VPN lines were not ready when the H1N1 immunization clinics opened, but were to be installed within two days from the start of the clinics. The use of the memory sticks was intended as a short term solution. However, even though the VPN lines were installed, each clinic site experienced problems in the transfer of information and so the use of the memory sticks continued and

became the primary way to communicate the required information between the community clinics and the main server at Regional Headquarters.

Under this process, each morning at the Regional Headquarters, a nurse would pick up a memory stick along with the vaccines for each clinic. The memory stick would contain the most recent copy of the immunization records held on file for all individuals immunized to date within the Region. Staff at the clinics required this information on site in order to ensure that they had up-to-date knowledge of the individuals who were coming back for second immunizations or to determine which immunization had been provided (H1N1 versus seasonal flu shot). As the nurse was responsible for securely transporting the vaccines to the clinics, it was thought that this would be a secure way to transport the memory stick to the clinic each day.

Upon arrival at the H1N1 immunization clinic, the nurse would provide the memory stick to a CIS staff member to begin the process of uploading the data to the local server at the clinic. At the end of the day, the CIS staff member would download all the information on the clinic's local server to the memory stick, returning it to the nurse to be merged with data held on the main server at Regional Headquarters.

My staff were further advised that some of the events leading up to and immediately following the loss of the memory stick had been captured by various security video cameras located around the Regional Headquarters building. There is a camera located outside the Shipping and Receiving department which has a motion sensor, and as such, captures activities in the vicinity when activated. In addition, the camera often picks up activities happening in the background.

On December 16, 2009, this video camera recorded the nurse, in the background, leaving Regional Headquarters with the immunization cart being pulled behind her and captured the nurse again when she was retracing her steps back to the main building, looking for the missing memory stick. The camera shortly afterwards captured another member of staff exiting the building and bending down to pick something up. Although the camera had been turned off at that point, because there was no activity occurring in the immediate Shipping and Receiving area, a witness who was outside at that time confirmed that they saw a staff member pick up a memory stick and place it on a rock next to the walkway. The witness, as well as the staff member who picked up the memory stick, were both interviewed. It was determined that the staff member who found the memory stick had placed it on the rock believing that someone would come back looking for it and notice it on the rock. Unfortunately, by the time the nurse retraced her steps, the memory stick was not found. My staff were advised that the above actions occurred within a four-minute timeframe.

The alarming failure of the Durham Health Department to have appropriate encryption in place raised an immediate concern with regards to ongoing H1N1 immunization clinics. To alleviate this concern, at our December 29, 2009 meeting, my office provided the Director for Technical Services in the CIS Department with a ready-to-deploy encryption software solution offered by CryptoMill, an Ontario-based company. We also put them in contact with this company, which specializes in protecting the privacy and security of data on laptops/desktops and all mobile storage devices through encryption technologies. Subsequent steps taken by the Durham Health Department and Durham Region, with regards to implementing encryption, will be discussed later in this Order.

4.0 ISSUES ARISING FROM THE INVESTIGATION

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

(A) Is the Medical Officer of Health of the Regional Municipality of Durham a "health information custodian" as defined in section 3(1) of the *Act* and were the nurse and CIS employee who provided the unencrypted memory stick 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 collect personal health information in compliance with Part IV 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 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*?

(F) Did the health information custodian comply with sections 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)?

(G) Did the health information custodian ensure that all agents were informed of their duties as required by section 15(3)(b) of the *Act*?

5.0 RESULTS OF THE INVESTIGATION

Issue A: Is the Medical Officer of Health of the Regional Municipality of Durham a "health information custodian" as defined in section 3(1) of the *Act* and were the nurse and CIS employee who provided the unencrypted memory stick 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:
>
> 6. A medical officer of health of a board of health within the meaning of the *Health Protection and Promotion Act*.
>
> …
>
> 8. Any other person prescribed as a health information custodian if the person has custody or control of personal health information as a result of or in connection with performing prescribed powers, duties or work or any prescribed class of such persons.

The written submissions provided to my office agree that the Medical Officer of Health is a "health information custodian" pursuant to section 3(1)(6) of the *Act*.

In addition, the submissions take the position that the Regional Municipality of Durham is a health information custodian pursuant to the *Act* and that:

> …the Medical Officer of Health and the Regional Municipality of Durham were both responsible for the health information collected, used, disclosed, retained or disposed of by agents on their behalf pursuant to section 17 of the Act.

Durham Region By-Law Number 51-2007 was provided as part of the rationale for this position. However, while the by-law states that the Regional Chair is designated as a health information custodian, no further information is provided as to how the Regional Chair or the Regional Municipality of Durham fit within the definition of health information custodian, which is set out in section 3 of the *Act*. In addition, we have not been provided with any evidence that the Regional Chair or the Regional Municipality of Durham were prescribed as health information custodians under the *Act* (e.g. as Canada Blood Services has been and as is set out in section 3 of Ontario Regulation 329/04 under the *Act*.). We note that there is no legal authority under the *Act* for designating or prescribing a person as a health information custodian by way of a local by-law.

Therefore, based on the above information, I find that Dr. Robert Kyle, the Medical Officer of Health of the board of health of the Regional Municipality of Durham, is the health information custodian (the Custodian) in this matter as defined in section 3(1)6 of the *Act*.

With regard to whether the nurse who lost the memory stick is an agent of the Custodian, section 2 of the *Act* defines an agent as follows:

> 2. In this *Act*,
>
> "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 of the *Act* states:

> (1) 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.

The submissions provided on behalf of the Custodian assert that the nurse who lost the memory stick was at all times an employee of Durham Region and was acting in a public health capacity such that she was an agent of the Medical Officer of Health.

Based on the above, I agree and find that the nurse is an agent of the Medical Officer of Health as defined in section 2 of the *Act*. With respect to this incident, she was therefore acting as an agent of the Custodian.

In addition to the information provided about the nurse, the written submissions go on to state that the employee responsible for encrypting the memory stick was at all times an employee of the Region performing duties in the Corporate Information Services Department and as such was an agent of the Region.

As I found above, in the same way that Durham Region is not a health information custodian pursuant to the *Act* in this matter, I do not agree that the CIS employee, in this instance is an agent of Durham Region.

However, as noted in the submissions, this incident was the result of the CIS employee providing the H1N1 immunization clinics with unencrypted memory sticks. The submissions acknowledge that unencrypted memory sticks were used in a process that involved personal health information being moved from one location to another.

Therefore, based on the above actions of the CIS employee and section 2 of the *Act*, I find that the CIS employee who provided unencrypted memory sticks to the H1N1 immunization clinics was an agent of the Custodian as he acted for or on behalf of the Custodian in respect of personal health information, even though he was an employee of Durham Region.

In summary, I find that both the nurse and the CIS employee are agents of the Custodian, as defined in section 2 of the *Act*. As a result, the Custodian is responsible for all personal health information collected, used, disclosed, retained or disposed of by these agents on his behalf, pursuant to section 17 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,
>
> (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,
>
> (f) is the individual's health number, or
>
> (g) identifies an individual's substitute decision-maker.

Identifying information is defined in section 4(2) of the *Act* as information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be used, either alone or with other information, to identify an individual.

The records at issue, contained on the memory stick, consist of information relating to 83,524 individuals who attended H1N1 immunization clinics in Durham Region. The information collected by the clinics and contained on the memory stick included personal demographic information and health information (client name, address, telephone number, gender, date of birth); health card number and expiry date (if a health card was provided); guardian information if the person was under the age of consent; health questionnaire answers provided by the client regarding their health history (e.g. pregnancy, allergies, cardiac or pulmonary diseases, or diabetes); date and location the client was vaccinated and the immunization received; and name of client's family doctor (if provided).

In addition to the above, an *H1N1 Vaccine Assessment/Questionnaire 2009* was provided as part of the submissions which indicated that information was collected on whether individuals were members of a priority group (H1N1 vaccine was originally available only to high risk groups and was not made available to the general public until some weeks into the immunization campaign).

Based on the above, I find that the records at issue are records of personal health information as defined in sections 2 and 4 of the *Act*. The submissions provided on behalf of the Custodian acknowledge that the memory stick contained records of personal health information.

Issue C: Did the health information custodian collect personal health information in compliance with Part IV of the *Act*?

Based on the information provided by the Custodian, the personal health information collected at the immunization clinics included personal demographic information and health information. As noted above, this information included client name, address, telephone number, gender, date of birth, health card number and expiry date (if health card provided); guardian information if the individual was under the age of consent; health questionnaire answers provided by the client regarding his or her health history (e.g., pregnancy, allergies, cardiac or pulmonary diseases, or diabetes); date and location the client was vaccinated and the immunization received; and name of client's family doctor (if provided). Personal health information was collected through the completion of a questionnaire. The questionnaire also requested detailed information about whether or not the individual fell within one of the priority groups.

The Custodian indicated that consent to the collection of personal health information was confirmed and documented prior to immunization. In obtaining consent for the collection of personal health information in Durham Region, the Custodian posted a privacy statement at all clinic registration areas and confirmed that this statement was read by the individual. In addition, the questionnaire included a notice that information was being collected under the authority of the *Health Protection and Promotion Act* R.S.O. 1990, c.H.7, part VII, subsection 91.1. for the purpose of providing immunization.

With respect to the collection of personal information, section 91.1(1) of the *Health Protection and Promotion Act* states:

> A medical officer of health may, subject to any conditions that may be prescribed in the regulations, directly or indirectly collect personal information for the purposes of this Act or for purposes related to administration of a public health program or service that is prescribed in the regulations. 2002, c. 18, Sched. I, s. 9 (11).

However, the requirements of the *Act* also apply to the collection. Specifically, section 29 of the *Act* states:

> A health information custodian shall not collect, use or disclose personal health information about an individual unless,
>
> (a) it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is **necessary** for a lawful purpose; or (emphasis added)
>
> (b) the collection, use or disclosure, as the case may be, is permitted or required by this Act. 2004, c. 3, Sched. A, s. 29.

Subsection 30(2) of the *Act* further limits the collection of personal health information as follows:

> A health information custodian shall not collect, use or disclose more personal health information than is reasonably **necessary** to the meet the purpose of the collection, use or disclosure, as the case may be. 2004, c. 3, Sched. A, s. 30(2). (emphasis added)

As previously discussed (under "Niagara Mass Immunization Data Collection") prior to the loss of the USB memory stick in Durham Region, in November of 2009, my office engaged in extensive discussions with the Ministry and two public health units in order to review the amount of information being collected at H1N1 immunization clinics, and the manner in which this information was being collected, to ensure consistency and transparency in the collection of personal health information.

In this matter, while the Custodian in Durham Region clearly has the authority to collect personal health information for the purpose of administering the H1N1 immunization program, it is not clear that *all* of the personal health information collected by the Custodian was *necessary* for that purpose.

The Custodian advised my office that personal health information was collected in accordance with the Ministry requirements, as set out in the data fields of the Niagara System. It was the Custodian's understanding that all of the information on the Niagara System provided by the Ministry was required to meet the purpose of the collection, use or disclosure. The Custodian explained that they initially questioned the Information Technology (IT) Support staff with the Niagara System as to whether or not they could delete certain fields if they did not deem that information necessary for providing immunizations. According to the Custodian, Niagara Support

staff advised them it was only possible to add in fields, not to delete them. Niagara Support staff added that if the Custodian elected not to include some of the fields as part of their collection of personal health information, Niagara would withdraw its IT Support. This has been confirmed with Niagara Region IT staff. As a result, the Custodian continued to collect personal health information which was not necessary for providing immunizations to the public.

However, agents of the Custodian advised that at each and every clinic, as well as on their website and through verbal communication with each patient, they made it clear to those consenting to the collection, use and disclosure of personal health information that they were not obliged to provide all the information requested in order to receive their immunization. As a result, some patients chose only to provide limited information. This supports the position that at least part of the personal health information that was collected by the Custodian was not necessary for the purpose of administering the H1N1 immunization program.

Further, although the Ministry narrowed the scope of the information being requested from public health units after December 2, 2009, the Custodian failed to recognize that an assessment of the personal health information being collected would be in order. Had the Custodian adequately assessed the necessity of the collection of personal health information, both at the outset of the implementation of the HIN1 immunization program and again when the Ministry issued its memorandum of December 1, 2009, rather than simply accepting the fields that were included in the Niagara System, the amount of personal health information that had been collected and subsequently transferred to the unencrypted USB memory stick would have been substantially reduced.

From our previous discussions with the Ministry and two public health units, it became clear that once the HINI vaccine was made widely available to everyone in the province, it was no longer necessary to collect information relating to priority groups. Although the client questionnaire used at HINI immunization clinics in Durham Region requested information relating to priority groups, the Custodian has not provided a rationale for continuing to collect this information once the vaccinations were made available to the general public.

In addition, although health card numbers are included as one of the data fields within the Niagara System, H1N1 vaccines are available to everyone, regardless of whether or not a health card number is provided. The Custodian indicated that the health card number was collected to serve as a unique identifier for clients. Accurate identification of individuals is important when recalling clients' histories during the course of administering both second doses and multiple vaccines.

While we agree that it is important to accurately identify individuals when providing health care, we have concluded from our previous discussions with other public health units that the health card number is not necessary for this purpose. In fact, most individuals can be accurately identified through their name and date of birth. Where individuals happen to have the same name and date of birth, additional demographic information such as address may be used. In

addition, the fact that individuals were immunized regardless of whether or not a health card number was provided further supports our view that health card numbers are not necessary for the purpose of administering immunization programs.

All health information custodians in Ontario should be aware that they are responsible for all of the personal health information that is collected, used and disclosed by all of their agents and electronic service providers on their behalf. They must clearly establish the purposes for which each type of personal health information is collected, used and disclosed by the custodian and ensure they have the appropriate legal authority for each collection, use and disclosure. In addition, all health information custodians must ensure that they do not collect, use or disclose personal health information if other information will serve the purpose, and that they do not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose. Personal health information should never be collected solely because it is needed to fill a data field in a software program the custodian has elected to employ, nor should personal health information be collected by a custodian for the purposes of or at the direction of another third party or in order to receive funding from a third party, unless the collection is authorized by the *Act*. Ultimate accountability for the appropriate collection, use and disclosure of personal health information always rests with the responsible health information custodian – it cannot be shifted to another party or an agent of the custodian.

Based on the above information and the representations made by the Custodian, I find that the Custodian did not limit the collection of personal health information to that which was reasonably necessary to fulfill the identified purposes, as required by the *Act*. Specifically, the Custodian has not provided a convincing rationale for collecting health card numbers or for collecting information pertaining to priority groups once the vaccine had been made available to the general public. Since the collection of this personal health information was not in compliance with the *Act,* the Custodian should immediately cease collection and securely dispose of this information. This will be addressed in my Order provisions.

Issue 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?

Section 13(1) of the *Act* states:

> 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.

The Custodian was asked to provide details as to the purpose for which the personal health information was transferred to the memory stick and the necessity for such a transfer. In addition, the Custodian was asked to describe what measures were taken to date, prior to and following the loss of the memory stick, to ensure compliance with Order HO-004, which clearly set out the standard to be followed for protecting person health information on mobile devices.

As noted early in this Order, the Custodian initially planned to use a VPN to transfer personal health information to and from eight community H1N1 immunization clinics and the main server at Regional Headquarters. However, due to technical difficulties, the back-up solution of using memory sticks was put into place and eventually became routine practice.

The Custodian advised that prior to the establishment of H1N1 immunization clinics and the corresponding use of the Niagara System:

> The Health Department has recognized the importance of protecting personal health information contained on mobile devices for many years. The use of encrypted laptops and USB keys was established with CIS in prior immunization campaigns and documentation of this requirement dates back to 2006. The Information and Privacy Commissioner/Ontario (IPC) Order HO-004 further heightened our awareness of the need for encryption and hardware recovery programs. Since the IPC Order HO-004, there have been numerous discussions between the [Durham Health Department] and CIS regarding data protection and hardware recovery software requirements.
>
> The use of a VPN network to transmit the information securely to and from each site was worked on prior to and throughout the campaign. The need to encrypt the data was identified at a meeting between the Health and CIS departments prior to the beginning of the campaign. The use of encrypted USB keys was established with CIS in prior immunization campaigns and was successfully followed.

The Custodian further advised that for previous seasonal flu clinics, they had been using the Mass Immunization Module (MIM), which included the encryption of personal health information.

Despite the above, the memory sticks used for the H1N1 immunization clinics were inexplicably not encrypted. In this regard, the Custodian stated that the employee who created the process for the use of the Niagara System in Durham did not follow the Region's procedures and created a process that did not include the encryption of data stored on the memory sticks. That employee, who had recently been hired, advised that he had not been informed by the Custodian that encryption was a requirement since data transfer was to occur using a VPN. But as we know, a VPN was not used.

I acknowledge that the Custodian had clearly turned his mind to the need for encryption and had, in the past, ensured that mobile devices used in support of seasonal flu clinics were strongly protected. However, as they say, the devil is in the detail. In the case of the H1N1 immunization clinics, apparently due to the lack of communication about the critical need for encryption, personal health information was placed on an unencrypted memory stick, that was subsequently lost. When the decision was made to use memory sticks, even as a stopgap measure, the required security safeguards should have been clearly communicated to the new employee. The failure to do this was unacceptable and constituted a clear violation of the *Act*.

I therefore find that the Custodian did not ensure that these records of personal health information were retained and transferred in a secure manner and that the Custodian did not comply with his obligations under section 13(1) of the *Act*.

I recognize that the Durham Health Department has been employing encryption on mobile devices in its seasonal flu clinics over the past years. However, the H1N1 and seasonal flu clinics are only a part of the work carried out by the unit. The Durham Health Department was unable to provide my office with assurances that mobile devices used to deliver other services were fully encrypted and that personal health information contained on those devices was protected. I am therefore concerned that a comprehensive approach to ensuring the security of mobile devices has not been taken at the Durham Health Department and will address this issue in my Order provisions.

It is important to acknowledge that, in response to this incident, the Custodian has indicated that H1N1 immunization clinics conducted in January 2010 will be working from a paper-based system for collecting personal health information. In addition:

> [Durham Health Department] staff will use one laptop to access previous immunization histories. The information on the laptop will be in "read only" format and will be encrypted. The laptop will be returned to the [Durham Health Department] by the clinic leader in a locked laptop hard case and be placed in the locked vaccine room until the next clinic. The nurse designated as the clinic leader will pick up the laptop and securely transport it in the nurse's vehicle to the clinic site. The laptop will be locked to the table at the site of the clinic using a combination lock. Only trained clinic leaders will be authorized to transport the laptop and they will be required to sign the laptop in/out from the vaccine room. As well, a process will be put in place to have signed tracking of the clinic laptops in the event that they are moved between the [Durham Health Department] and the Departments.

Even more significant, in my view, is the willingness of Durham Region, which provides technical support to the Durham Health Department, to move quickly to address its deficiencies in terms of the security of personal information on mobile devices. The fact that deficiencies exist became apparent during this investigation. For example, it became clear that a large number of the laptops in use by Regional staff in departments other than the Durham Health Department are not encrypted. Also, given that the Durham Health Department received the unencrypted memory stick from a CIS staff member, one can easily infer that the encryption of memory sticks is not standard practice among all departments of Durham Region.

An excellent resolution to these issues is presently under development. As mentioned earlier in this Order, at a meeting on December 29, 2009, my staff provided Durham Regional staff with a ready-to-deploy encryption software solution on portable media offered by CryptoMill, an Ontario-based company. CryptoMill has volunteered their enterprise encryption solution for use as an interim measure until the Durham Health Department has put in place a permanent solution. Within days of this data breach, CryptoMill and Durham Region began a series of meetings to discuss how to address the encryption needs of, not only the Health Department, but the entire corporate administration of Durham Region. On January 11, 2010, a pilot project of an encryption solution commenced. This pilot involves the deployment of encryption to fully protect any removable storage media within the Durham Health Department. If successful, this deployment will be rolled out throughout all of Durham Region. I want to gratefully recognize

the commitment of Durham Region, led by Corporate Information Officer, Ray Briggs, to this ongoing work. I applaud these efforts.

Durham Region, as an institution under the *Municipal Freedom of Information and Privacy Act*, has a legislated responsibility to protect all personal information in its custody or control, not only personal health information. Order HO-004 set a standard for health information custodians regarding the protection of personal health information on mobile devices. That standard is equally applicable to any municipal or provincial government institution that collects and retains personal information. As a result, I will be recommending that Durham Region continue its efforts in this regard.

This investigation has also raised a concern with regard to the data security practices in place at the other 35 public health units in the province. Although aware of Order HO-004, the Durham Health Department still had this regrettable incident when operating its HIN1 immunization clinics and could not provide us with assurances that all mobile devices being used by its staff were encrypted. While my Order provisions will provide greater protections for the residents of Durham Region, such protections must be in place province-wide. This incident has left open the possibility that other health units are not following Order HO-004 and that the personal health information of Ontarians, whether collected by health units through the delivery of HIN1 immunization clinics, seasonal flu clinics or other services, may not be sufficiently protected. This must be rectified immediately.

While I appreciate that neither the Ministry nor the Chief Medical Officer of Health have the ability to require the 36 boards of health to perform certain functions, they have a significant and important role to play in providing leadership to these organizations. Similarly, while boards of health are independent and, in the case of the HINI immunization clinics, were free to determine how they were to proceed, it is clear that they look to the Ministry for guidance. This is confirmed by the Custodian's representations. The Durham Health Department willingly adopted the Niagara System that was financially supported by the Ministry and did not feel they were in a position to alter or modify the system provided to them.

In addition, despite the involvement of the Ministry in the development of the Niagara System, significant privacy issues relating to the distribution of the vaccine were overlooked. For example, as noted earlier in this Order, the amount of personal health information that public health units were asked to collect was overly broad for the purposes of providing vaccinations. No one from the Ministry consulted with my Office about this matter. Had they done so, this problem could have been rectified at that time — right from the outset.

Given the leadership role that the Ministry and the Chief Medical Officer of Health should play in ensuring that all 36 public health units are sufficiently protecting personal health information contained on mobile devices, I will be making a number of recommendations. These will include recommending that the Ministry, in conjunction with the Chief Medical Officer of Health, ask each public health unit to conduct a review of its practices and procedures with regard to encrypting personal health information on mobile devices. Further, I will recommend that they request the medical officer of health for each public health unit to provide them with an attestation that no unencrypted personal health information is being transported on mobile devices. Finally, I will

recommend that the Ministry, in conjunction with the Chief Medical Officer of Health, audit a representative sample of the practices of public health units.

Issue E: 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*?

Section 10(1) of the *Act* states:

> 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.

Information practices are defined in section 2 of the *Act* to mean "the policy of the custodian for actions in relation to personal health information." The definition refers to "when, how and the purposes for which the health information custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information" and "the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information."

In Order HO-004, I reviewed the need for health information custodians to ensure that their information practices are current and reflective of changing operational requirements:

> Health information custodians should review their information practices regularly to ensure that they remain appropriate for their operations. As the health information custodian's operations evolve and grow, and as a result of the introduction of new information technology, it is important to update information practices to reflect these changes. A health information custodian should take steps to ensure that the contents of its policies and procedures are kept current to reflect actual practices. In addition, a health information custodian should keep abreast of developments relating to safeguards to ensure that they comply with the *Act*.
>
> In addition, when adopting policies and procedures, a health information custodian needs to ensure that staff members and independent contractors are made aware of new policies and procedures by proper notice, either through the use of the internal mail system, electronic mail and/or educational sessions.

In its written representations, the Custodian takes the position that the Custodian's information practices were in compliance with sections 10(1) and (2) of the *Act*. Specifically, the representations state:

> The policies and procedures of the Region and the CIS department in particular dictated that all USB keys used for the purposes of carrying and containing personal information were to be encrypted. The Region has run several successful seasonal flu vaccination clinics using a program created in house by the Region's CIS staff. This program was written in such a way that no USB key could be used to transport any data without first being encrypted. The program itself was created in this manner to comply with all Regional policies regarding the protection of personal health information. In this instance, the employee who created the process for the use of the Niagara [System] in Durham did not follow the Region's policies and procedures and created a process that did not include the encryption of USB keys.

I have reviewed the relevant policies and procedures provided by the Custodian and, with respect, simply cannot agree with the conclusion that these policies and procedures comply with section 10(1) of the *Act*. For example, Durham Region's *Data Protection Policy*, is presumably applicable to data held by the Medical Officer of Health. While the policy states that "confidential" information must be encrypted prior to transmission over untrusted networks such as the Internet, the policy is silent on the need to encrypt confidential information contained on mobile devices. Further, the definition of "confidential" refers to "systems information, password lists, and employee data" leading me to believe that the *Data Protection Policy* was not developed specifically to address the protecting of personal health information.

The policies of the Durham Health Department itself are much more relevant and demonstrate a significant problem. At the time of the incident, the applicable policy of the Durham Health Department was dated April, 2002 and entitled *PC/DESKTOP SECURITY*. As the title indicates, it was developed without considering the application of security to mobile devices. In addition, any mention of encryption was absent. This policy would not provide staff with any guidance on how to secure personal health information being transported on a mobile device, such as a laptop or memory stick.

The Durham Health Department had started to review the *PC/DESKTOP SECURITY* policy prior to the loss of the memory stick on December 16, 2009. I was provided with a draft version dated October, 2009, entitled *COMPUTER/LAPTOP/TABLET SECURITY*. The policy states that IT staff will install encryption software on all health department computers, which includes computers, laptops and tablets. The policy further states that where encryption software cannot be added to existing laptops, staff will ensure that they are not used for sensitive or confidential information. Regrettably, this policy was not updated prior to the opening of the H1N1 immunization clinics.

This policy has undergone further revisions as a result of this incident. The December 2009 version, approved December 31, 2009, which postdates the loss of the memory stick, now includes storage devices. In addition, the revised policy states that information technology equipment taken off site must be safeguarded by being secured out of public view in an employee's locked

vehicle, or locked in a secure area within the office. Outside of regular work hours, equipment must be secured in an employee's home if taken off site, or locked in a secure area within the office. When using a mobile storage device, such as a memory stick, staff will ensure that the device is encrypted and placed on a lanyard (a braided fabric cord worn around the neck), as well as ensuring that the device is secured during transport.

The policies that were in use at the time of the incident were clearly inadequate. As indicated above, the most relevant policy of the Durham Health Department did not even contemplate mobile computing or storage devices. I understand that the Durham Health Department may have operated on the understanding that laptops and memory sticks had to be encrypted. I also appreciate the fact that the Durham Health Department had run successful seasonal flu clinics in the past using encrypted devices, and applaud them for this. However, the fact remains that the memory stick involved in this incident was not encrypted. In addition, had a CIS or Durham Health Department staff member consulted the applicable policies and procedures, no helpful guidance on how to handle personal health information outside the office environment would have been readily available.

I am also cognizant of the fact that the Durham Health Department has revised its policies to conform with the reality of mobile devices. However, I am still not satisfied that the latest version of the policy provides enough specific guidance regarding how and when encryption should be deployed.

Order HO-004 sets out the minimum standard for what I expect from all health information custodians in Ontario regarding the protection of personal health information. The Custodian involved in this case clearly did not comply with that standard. Anything less than the minimum standard created in Order HO-004 falls short and is unacceptable.

Finally, 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. It is clear that the vital step of implementing information practices did not take place in this case.

As such, I find that the Custodian's information practices do not meet the requirements of section 10(1) and (2) of the *Act*.

Issue F: Did the health information custodian comply with sections 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)?

Section 12(1) of the *Act* states:

> 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* states:

> 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 D and E, 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*.

With respect to the notification requirement set out in section 12(2) of the *Act*, the Custodian provided a copy of the letter sent to the affected individuals and confirmed that all notification letters, with the exception of those with incomplete address information such as missing postal codes, have been mailed out. Staff continue to work on identifying incomplete information to confirm mailing addresses for the remaining letters.

In addition, the Durham Health Department issued a News Release on December 21, 2009, to advise the public of this breach.

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

However, based on the circumstances of this case, I am of the opinion that further action is required by the Custodian. To date, close to 84,000 individuals have been notified that their personal health information, collected at H1N1 immunization clinics, has been lost. This has undoubtedly raised a great deal of trepidation in the Durham community and fear that this information will be put to malicious uses, such as identity theft. Indeed, as mentioned in the Background section of this Order, my office has been contacted by a number of individuals who expressed their anger and disbelief that this was allowed to happen. Citizens will also be

anxious to learn the facts of this incident and what steps have been taken by the Custodian and Durham Region, to ensure that a similar incident does not happen again.

In order to reassure those individuals whose personal health information was lost that strong action has been taken and to allay their fears, I will therefore be recommending that the Custodian take steps to publicize the issuance of this Order and to inform citizens where they can obtain a copy.

Issue G: Did the health information custodian ensure that all agents were informed of their duties as required by section 15(3)(b) of the *Act*?

Section 15(1) of the *Act* states:

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

Section 15(3)(b) of the *Act* states, in part:

> 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*;

In its submissions, the Custodian advised that staff training on the *Act* occurred at two Durham Health Department meetings in 2007. A follow-up e-mail was sent asking managers to have staff not in attendance review the training information online and complete a *PHIPA Acknowledgement Form*. In addition, all new staff hired by the Durham Health Department received training on the *Act* at the Durham Health Department orientation. Temporary administration clerks hired for immunization clinics received training on the *Act* during orientation to the immunization clinics.

Copies of the training presentation slides, the minutes of the meeting where the training occurred, the e-mail follow-up, the online training and the *PHIPA Acknowledgement Form* were provided to my office.

Also included with this material was the actual *PHIPA Acknowledgement Form* that was signed by the nurse who lost the memory stick, which shows that she had received appropriate training. However, with respect to the CIS employee involved, the Custodian advised that he had only commenced employment at Durham Region on September 16, 2009, and confirmed that he had not received any training on the *Act* at the time of the incident.

Based on the above, despite the Custodian's best efforts, I find that the Custodian did not comply with 15(3)(b) of the *Act*, as the CIS employee was not adequately trained and ultimately failed to encrypt the memory stick involved. However, in view of the extensive training regime in

place for Durham Health Department staff, I have concluded that it is not necessary to include this as an Order provision.

Tangentially, similar to my concern that encryption practices across the province may not meet an acceptable standard, 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. Again, I believe that there is a leadership role to be played by the Ministry. The Ministry is best positioned to ensure that a consistent level of training is provided to all public health unit staff, regardless of their location. As a result, I will be recommending that the Ministry provide resources to the Chief Medical Officer of Health for the development of training materials to ensure that all public health unit staff are aware of the need for proper safeguards for personal health information stored on all mobile devices.

6.0 SUMMARY OF FINDINGS

I have made the following findings in this review:

1. The Medical Officer of Health of the Regional Municipality of Durham is the "health information custodian" as defined in section 3(1) of the *Act* and the nurse and the CIS employee who provided unencrypted memory sticks to the H1N1 immunization clinics, 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 section 30(2) of the *Act* as it did not limit the collection of personal health information to that which was necessary to fulfill the identified purposes, as required. Specifically, the Custodian has not provided a convincing rationale for collecting health card numbers and information pertaining to priority groups after the H1N1 vaccine was made widely available to the general public.

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 sections 10(1) and (2) of the *Act* as it did not have information practices in place that comply with the requirements of the *Act*.

6. 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. The Custodian did comply with section 12(2) of the *Act* by fulfilling its obligation to notify affected individuals.

7. The Custodian did not comply with section 15(3)(b) of the *Act* as the agent involved in administering the Niagara System was not adequately trained in his role or his obligations under the *Act*.

7.0 ORDER

1. I order the Custodian 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.

2. I order the Custodian to 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 Order Provision 1, and to consult with my office prior to finalizing those information practices.

3. I order the Custodian to take the necessary administrative steps to ensure that H1N1 immunization clinics cease collection of the health card numbers of individuals attending these clinics, as well as personal health information pertaining to priority group status.

   Order Provision 3 does not affect the ability of the Custodian to collect personal health information relating to priority group status in the event that such status is relevant to receiving H1N1 vaccine at future immunization clinics.

4. I order the Custodian to take the necessary administrative steps to ensure that health card numbers collected from individuals who have attended H1N1 immunization clinics are securely destroyed as well as any personal health information relating to priority status collected from individuals after the H1N1 vaccine was made widely available to the general public.

In order to verify compliance with this Order, I require that the Custodian provide me with proof of compliance by **February 16, 2010**.

8.0 RECOMMENDATIONS

I recommend the following:

Medical Officer of Health for the Regional Municipality of Durham

1. That the Medical Officer of Health for the Regional Municipality of Durham take the necessary steps to inform the public about the issuance of this Order and provide information on how to obtain a copy. Further, I ask that this include placing advertisements in local newspapers in the Durham Region, and directing the public to the IPC website to obtain a copy of the Order.

Regional Municipality of Durham

2. That the Regional Municipality of Durham develop and implement a comprehensive corporate policy for mobile devices (i.e., laptops, memory sticks, PDA's) to ensure that, to the extent that personal information must be transported on those devices, it is strongly encrypted.

Ministry of Health and Long-Term Care

3. That the Ministry of Health and Long-Term Care, in conjunction with the Chief Medical Officer of Health, undertake the following:

    - Request each public health unit to 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;

    - Request that each medical officer of health in the province provide the Ministry with an attestation that no unencrypted personal health information is being transported on mobile devices; and

    - Audit a representative sample of public health units to verify the information provided by the medical officers of health.

4. That the Ministry of Health and Long-Term Care provide resources to the Chief Medical Officer of Health for the development of training materials to ensure that all public health unit staff are aware of the need for proper safeguards for personal health information stored on mobile devices.

9.0 COMMISSIONER'S MESSAGE

Health information custodians in Ontario are required under the *Act* to take reasonable steps to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure. In 2007, following the loss of a laptop containing personal health information, I sent a clear message warning all custodians against storing personal health information on mobile devices, that are especially vulnerable to both loss and theft. In Order HO-004, I outlined a new standard to be followed – a multi-layered approach to guard against unauthorized access to personal health information stored on mobile devices.

It is always preferable to *avoid* storing any personally identifiable health information on mobile devices. However, where personal health information must be stored on such devices, the following measures are necessary:

- only the *minimal amount* of information necessary should be stored, and for the *minimal amount of time* necessary to complete the work;
- whenever possible, personal health information should be *de-identified or coded*, in a manner such that the identities of the individuals whose personal health information is stored on the device could not be readily ascertained if the information were accessed by unauthorized persons;
- if the information is coded, the code that is needed to unlock the identities of individuals should be stored separately on a secure computing device, such as a central server in a health care facility;
- the use of *strong password protection*; and, most important,
- the use of *strong encryption*.

The *Act* requires custodians to notify individuals if their personal health information is lost, stolen or accessed by unauthorized persons. Consequently, privacy breaches tend to be both time-consuming and costly, and often result in irreparable damage to a custodian's reputation and image. 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.

Multiple factors may contribute to the failure to adequately safeguard personal information. First, there may be a lack of understanding about the vulnerabilities, threats and risks to the information stored on mobile devices, or a lack of awareness about what constitutes reasonable safeguards for personal health information stored on such devices. Second, there may be challenges in implementing enterprise-wide solutions that allow custodians to effectively manage

and control the manner in which all of their agents and electronic service providers collect, use, disclose, retain, transfer and dispose of personal health information on their behalf. Third, while this is difficult to believe, some custodians may have interpreted Order HO-004 narrowly as applying only to mobile computing devices such as laptops and personal digital assistants, without recognizing that other portable data storage devices, such as USB memory sticks, pose similar risks. The stolen laptop that resulted in HO-004 and the lost USB memory stick resulting in the current Order are instances of a growing class of security and privacy problems, namely data leakage and data loss associated with all portable storage devices. My office is taking steps to ensure that all of these issues are addressed.

As the health sector moves towards electronic health records and electronic systems of personal health information, public confidence in custodians' ability to protect all types of health records is essential. Privacy breaches stemming from the use of technology, without the necessary privacy and security safeguards such as encryption, will inevitably be viewed as harbingers of the state of privacy once the health sector makes the transition to electronic health information. In my view, this is completely understandable. After all, if custodians cannot be trusted to protect the personal health information stored on a simple portable device such as a USB key, how will they ever manage to protect the massive amounts of personal health information that will eventually reside within complex systems of interoperable electronic health records?

It is vital that custodians recognize that any breaches stemming from the improper implementation of information technologies will not only be costly for the responsible custodian, but will also reinforce skepticism about the health sector's ability to protect privacy in context of ehealth, in general. Increased skepticism will likely have a chilling effect on the acceptance and adoption of all types of new health information technology, including electronic health records. Given recent setbacks in the ehealth agenda in Ontario, additional barriers or delays are the last thing the health sector needs at this point in time. Therefore, it is essential that all custodians demonstrate both their commitment and their capacity to protect personal health information stored in all formats, *now.* Otherwise, the transition to the use of electronic health records will be far from smooth.

In recognizing the broader implications of large scale breaches of health information and the need to ensure that immediate steps are taken to prevent avoidable breaches involving mobile devices, I approached the Ministry of Health and Long-Term Care. They have committed to work together with my office to develop a communications strategy to help ensure that the entire health care sector in Ontario adopts reasonable safeguards to protect personal health information stored on all types of electronic devices. As a first step in this strategy, I contacted the Chief Medical Officer of Health for the province of Ontario who issued a memo to all medical officers of health, warning about the need to encrypt personal health information on portable devices such as USB memory sticks. A more detailed strategy for promoting awareness and compliance among all health information custodians is currently under development and will be finalized early in 2010.

However, enhanced awareness is only part of the solution. As storage capacity increases while costs decrease dramatically, portable storage devices are proliferating in information intensive sectors, such as the health sector. In this environment, it will be a challenge for health information custodians to establish effective management and control over all of their data resources, as well as maintaining effective accountability for the standards required under the *Act*, and widely expected by the public.

As I have stated over the years, in light of the proliferation of new information and communication technologies, the future of privacy requires a comprehensive and proactive approach, which I have called *Privacy by Design*, whereby both privacy and security are effectively baked into the information eco-system, end-to-end, and throughout the entire data life-cycle, from initial collection through to final disposal.

While encryption is a key component of any security solution for protecting health information on portable devices, it must be deployed in a holistic and proportional manner in order to be truly effective. Depending on the operating context, some encryption solutions are better than others. Those that are added on, after the fact, requiring users to actively encrypt files by creating passwords or launching a software program every time that health information is stored on a portable device, may be less effective than other encryption solutions. Weak or stolen passwords effectively negate the potential security benefits of encryption. Confusing or complex software interfaces and protocols will also result in users abandoning secure systems and resorting to insecure "workarounds." Users also may be unaware that when encrypted information is transferred from one storage device (e.g., laptop computer) to another (e.g., a USB key), the encryption does not necessarily accompany the data. Once the data is intentionally or unintentionally decrypted back to plaintext, it is out there in plain view, becoming vulnerable to a wide range of unintended uses.

Doing away with mobile devices entirely by locking down all USB ports, in favour of the exclusive use of secure channels and "thin clients," is another approach that may be feasible in some instances but not others. Thin clients, sometimes described as "dumb terminals," are display and input devices which do not process data and input locally, but rather transmit input to a computer to which they are connected and display the resulting output. They often have limited local data storage and output capacities. Since the vast majority of the processing of information is done centrally in such systems, the security risks are generally confined to the central server. However, while it may be easier to manage the security risks, establishing and maintaining secure channels and thin clients tends to be operationally complex and costly to the enterprise, requiring employees to manage identification and authentication credentials in a consistently secure way. Additionally, locking down USB ports across an enterprise may rob an organization of the benefits of connecting other useful, risk-free devices to those ports, such as a mouse or keyboard.

Ideally, organizations should implement enterprise-wide encryption solutions that would only permit the use of authorized portable storage devices to connect to specifically-authorized USB ports, where the encryption is both automatic and seamless. Only devices with authorized USB ports would be able to view, access and decrypt the data stored on an authorized portable storage device. Thus, in the event that an authorized portable storage device was lost or stolen, any

personal health information stored on the device would be inaccessible to anyone who found it. Further, it would simply not be possible to use an unauthorized mobile device with such a protected system. The management of this type of arrangement would have to be centralized, easy to set up and administer, and, ideally, low in cost. In addition, all transactions would also need to be logged.

A local Ontario company, CryptoMill, has developed such an enterprise-class security solution that offers this degree of functionality. Their solution called *SEAhawk*, allows organizations to effectively lock down information assets to registered devices only, such as USB memory sticks.

Had such a solution been implemented in Durham Region, the personal health information contained on the USB memory stick that was lost would have been encrypted in a manner that would have locked out all unauthorized parties, only allowing an authorized computer to decrypt it. Further, any files stored on the USB memory stick would essentially be *invisible* to anyone who found it or stole it. Anyone, including staff, plugging the USB memory stick into their own computer would either find an encrypted vault – an invisible directory, or else be prompted to format an unrecognized drive, effectively erasing its contents.

If an encrypted USB memory stick was lost, there would be no cause for alarm on the part of the organization, which would have a high degree of confidence that the stored data would not be compromised. There would be no need to invoke the time-consuming and expensive breach management process involving notification, investigation, and remediation.

To their credit, both CryptoMill and Durham Region have been working together non-stop to apply the SEAhawk encryption solution throughout the Durham Region. With the release of this Order, its adoption will be well underway.

Privacy by Design is systemic, embedded, and proactive in nature, thereby serving to prevent privacy mishaps before they occur. It comes *before* the fact of a data breach, not after. While it is true that we cannot eliminate human error, we most certainly *can* eliminate personal information from being revealed, in the process. Human error, in this instance, is not an acceptable excuse. While the loss of a USB memory stick may not have been prevented, the loss of personally identifiable data certainly could have been. Don't blame human error – blame the lack of encryption of easily lost or stolen mobile devices.

January 14, 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
Website: www.ipc.on.ca
Email: info@ipc.on.ca