Information and Privacy Commissioner/ Ontario

ORDER HO-004

Ann Cavoukian, Ph.D.
Commissioner
March 2007

BACKGROUND

On January 15, 2007, the Office of the Information and Privacy Commissioner/Ontario (IPC) was contacted regarding a stolen laptop computer belonging to the Hospital for Sick Children (SickKids). The laptop contained the personal health information (PHI) of current and former SickKids patients. The IPC immediately commenced an investigation of this incident, pursuant to the *Personal Health Information Protection Act* (the *Act*).

NATURE OF THE INCIDENT

On January 4, 2007, a physician at SickKids, who is both a clinician and a researcher, left the hospital with one of its laptop computers, with the intention of taking it home to analyse research data that was stored on it. However, the physician did not go directly home. Instead, he parked his vehicle, a minivan, in a Toronto Parking Authority parking lot in downtown Toronto between the hours of 7:30 p.m and 11:00 p.m. Given that the minivan had no trunk, he placed the laptop computer between the front seats and covered it with a blanket. When he returned to his vehicle, the front passenger window had been broken and the laptop was gone. The physician immediately filed a vehicle break-in report with the Toronto Parking Authority and, on the Toronto Police Service's advice, filed a police report the following morning. To date, the police have not recovered the laptop computer.

On January 5, 2007, the physician notified his department head and the Chair of the Research Ethics Board, who, in turn, notified SickKids' Privacy Contact on January 9, 2007. On January 10, 2007, members of the senior management team met, where it was determined that the incident warranted action as set out in SickKids' policy entitled "*Management of Critical Occurrences*" (MCO). Implementation of this policy involved notification of the appropriate people, including patients and their families, and conducting an internal investigation in order to identify systems-related issues and make recommendations to prevent a reoccurrence, assign responsibilities, and establish timelines for implementation.

One of the objectives of the internal investigation was to determine the nature of the data contained on the laptop computer. SickKids advised the IPC that the data consisted of Excel spreadsheets containing the personal health information (PHI) of approximately 2,900 current and former SickKids patients involved in five prospective research studies and five retrospective research studies. Approximately 157 patients are involved in the prospective studies and approximately 2,700 patients are involved in the retrospective studies.

A prospective study requires the patient's consent, as the patient receives treatment during participation in the study. As such, the patient is aware that his/her PHI is being used for research purposes. A retrospective study generally consists of a review of the records of past patients. A research ethics board may, under certain circumstances, approve a waiver of the consent requirement for such studies. The Research Ethics Board (REB), established by SickKids, had approved all ten studies and the waiver of the consent requirement for all five retrospective studies.

The amount of information pertaining to each patient varied, but all cases involved identifiable PHI. At a minimum, the patient's name and SickKids Hospital Number was included on the spreadsheets. In addition, in each case, some information relating to the patient's medical condition was included in the data, such as vascular testing measures, operative dates, surgical details, and/or diagnoses. In some, but not all cases, very sensitive information was also included, such as answers provided in interviews and questionnaires relating to morbidity and mortality details, perceptions of quality of life, drug therapy, and patients' HIV status. The physician was one of seven co-investigators involved in the research studies, and, in two studies, was the principal investigator. Some of the patient information in one of the retrospective studies had been provided to SickKids by another hospital, the University Health Network (UHN), who was collaborating with SickKids on the study. All of the patients in the retrospective studies had transitioned from childhood to adulthood, 350 of whom were treated at UHN.

All of the data stored on the laptop was also saved on SickKids' main server. The only laptop security was an eight character alpha numeric login password. No encryption of any data had been enabled, at either the file or disk level. At the time of the incident, remote encrypted access to PHI in shared folders was available to researchers through standard commercial software via a Virtual Private Network (VPN), and to clinicians for access to clinical applications through commercial software called Citrix™. SickKids acknowledges that the researcher could have accessed this data remotely, which would have eliminated the need to remove it from the hospital on the laptop computer. SickKids also acknowledges that, in this particular case, the research data needed did not have to be accessed in identifiable form.

CONDUCT OF THE REVIEW

The IPC was initially advised of the theft of the laptop on January 15, 2007. Additional information was provided by SickKids in meetings with the IPC on January 26, 2007 and February 15, 2007, by way of a written report dated February 1, 2007 submitted to the IPC, and by way of written submissions dated March 2, 2007, in response to the IPC's request for written submissions.

As a result of the incident and as part of its MCO policy, a number of steps are being taken by SickKids to prevent a reoccurrence of this type. A review of its current policies and practices regarding portable computing devices, the use of encryption, and remote access is presently underway. As a preliminary precaution, an alert was sent out to staff members via the hospital's intranet "daily news" and "tip of the day" that stated:

> Any identifiable patient information must not leave the hospital, whether the material is "physical" (e.g. health record or x-ray) or "electronic" (e.g. on a laptop or flashcard). This includes research databases with identifiable patient information. Please note that it is a breach of hospital policy to have identifiable patient information leave the premises of the hospital. Please make sure that none of your electronic materials contain identifiable patient material.

SickKids' Privacy/IT/Risk Working Group met to discuss theft and preventative precautions, including a discussion of the issue of providing easier access to the central servers to lessen the use of "roaming devices."

In addition, consultation with the other research investigators took place to determine the most appropriate method of patient/family notification, and consultation with representatives of UHN took place to obtain patient contact information.

SickKids' REB has now mandated that all PHI stored and used for research purposes must be de-identified through the use of unique identifiers that cannot be traced back to a particular patient without the use of a legend to "crack" the code. The REB and the Clinical Research Office are planning to conduct random audits to ensure compliance and are contemplating penalties for those researchers who do not comply with the new process.

SickKids' Information Technology (IT) department is also seeking proposals from vendors relating to encryption software that can be effectively used on endpoint devices.

With respect to patient notification of the privacy breach, all active patients, that is, those who have been seen at SickKids within the last two years, for which SickKids has current contact information, have been notified of the incident by way of a written letter from SickKids. In those cases where the information contained on the laptop computer was of a sensitive nature, the patients and their families are being notified of the theft in person, at clinic appointments. It is worth noting that approximately one third of the patients affected by this incident are deceased. In addition, on March 1, 2007, SickKids issued a press release, which is also posted on its Internet site.

The hospital provided to the IPC copies of its *IT Strategic and Action Plans* and a number of policies and procedures that relate to the confidentiality and privacy of both personal information and PHI, theft/loss prevention and reporting, computer information security, clinical systems education, ethical conduct of research, and consent issues in research.

I would like to acknowledge the full cooperation given to my staff by SickKids during the course of this investigation. Staff of the hospital was at all times fully engaged in ensuring that a comprehensive investigation was completed and that meaningful measures are put into place to prevent a reoccurrence of this type of incident. I have nothing but praise for the cooperation extended.

ISSUES ARISING FROM THE REVIEW

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

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

(B) Is SickKids a "health information custodian" as defined in section 3(1) of the *Act*?

(C) Did SickKids, as the health information custodian, comply with sections 12(1) and 12(2) of the *Act*?

(D) Did SickKids, as the health information custodian, comply with section 13(1) of the *Act*?

(E) Did SickKids, as the health information custodian, comply with sections 37(1)(j) and 37(3) of the *Act*?

(F) Did SickKids, as the health information custodian, comply with section 10(1) of the *Act*?

RESULTS OF THE INVESTIGATION

Issue A: 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, or
>
> (f) is the individual's health number.

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 data stored on the stolen laptop consisted of the name and hospital number of each patient/research subject and is, therefore, identifiable. In addition, in each case, some form of clinical information about the patient was included, such as testing dates and measures, and diagnoses, and in some cases extremely sensitive PHI was included, such as HIV status, morbidity and mortality rates and drug therapy. Each patient included in the research study is currently a patient at SickKids or was a patient at some point in the past. A person reading the data would be able to ascertain that the individuals, who are named, had health issues that were diagnosed and/or treated at SickKids, therefore meeting the criteria for PHI as set out in the *Act*.

I therefore find that the information stored on the laptop computer consists of records of personal health information as defined in sections 2 and 4 of the *Act*. The hospital does not dispute this finding.

Issue B: Is SickKids a "health information custodian" as defined in section 3(1) of the *Act*?

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

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

I find that SickKids is a health information custodian, as it is the person who operates the hospital, which is a hospital within the meaning of the *Public Hospitals Act*. In addition, SickKids had custody and control of the PHI, as a result of both providing treatment to the affected individuals and conducting research utilizing the PHI of the affected individuals. SickKids therefore meets the definition of custodian as set out in section 3(1)4i of the *Act*. The hospital does not dispute this finding.

Issue C: Did SickKids, as the health information custodian, comply with section 12(1) and (2) of the *Act*?

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

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

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

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

Section 12(1) of the *Act*

Based on information provided by SickKids, namely the fact that the physician was able to remove identifiable PHI from SickKids' premises and store it on a laptop computer with only a single level password and in unencrypted form, I am not satisfied that SickKids has taken steps that were reasonable in the circumstances to ensure that the PHI in its custody or control was protected against theft, loss and unauthorized use or disclosure, as required under section 12(1) of the *Act*.

SickKids provided the IPC with copies of its *IT Strategic and Action Plans*. The Strategic Plan was last updated in February 2004 and states, in part:

> …security is an underlying principle of electronic access, thus security of the infrastructure is of paramount importance. The correct approach to security is a multi-layered approach with each layer offering an incremental level of access to the core – the electronic data itself. We will continue to apply this approach and employ best security practices at each layer of the infrastructure.

The plan illustrates the building blocks of the IT infrastructure with a diagram, depicting the network, servers and storage, common application enablers and access devices. Laptop computers are considered access devices. While the Strategic Plan clearly envisions the security of health information, it is limited in that it does not set out how the proposed security goals will be implemented on a hospital-wide basis.

Similarly, SickKids' IT Action Plan, updated in September 2006, only sets out the steps that will be taken to ensure access to PHI by clinicians. For example, the hospital will "provide easy, secure and reliable remote access to clinical, research and education data," and indicates that

the hospital will "continue the standardization of desktops and implement laptop standards to better support the recovery process." The document appears to place importance on improving access to PHI, appropriately so in my view. However, equally appropriate matching efforts to ensure the security and privacy of that PHI, are lacking.

SickKids has a number of general policies that make reference to the security of PHI and/or personal information. For example, the policy entitled *Privacy of Personal Information* states:

> Security safeguards appropriate to the sensitivity of the information will protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. SICKKIDS will protect personal information regardless of the format in which it is held. The methods of protection include physical, organizational and technological measures.

In addition, its policy entitled *Confidentiality of Information* indicates that:

> [the] removal of confidential information in any form from the Hospital premises is discouraged and must comply with established practices. Anyone removing confidential information is accountable for protecting such information until it is safely returned to the Hospital.

The policy entitled *Computer Information Security* states that:

> …computers and data can be accidentally destroyed or stolen. It is the responsibility of all users to protect the information stored on their personal computers. The more confidential and sensitive the information, the more comprehensive the measures to protect it must be taken.

The policy then provides examples of security measures, such as locking laptop computers out of sight when not in use, storing confidential information on a secure system with password access restrictions, using password protection and/or encryption on disks, and encrypting confidential information that is electronically transmitted over public networks such as the Internet. There is also a policy entitled *Theft/Loss Prevention and Reporting,* which states that laptop computers are to be stored in secured cabinets. Finally, SickKids has a *Workstation Software* policy that sets out the types of permitted and prohibited software on workstation and notebook computers. There is no reference to encryption in this policy.

Although the policies provided to the IPC by SickKids recognize the risks involved with identifiable PHI contained on laptop computers, they do not provide specific guidance as to how to reduce, or indeed, eliminate the risk by ensuring the security of the PHI. For example:

- the removal of confidential information from the facility is not prohibited, rather it is only "discouraged;"
- although the policies and procedures recognize that appropriate security safeguards are necessary, specific guidance is not provided as to what measures must be taken; and

- a variety of security measures are identified, however minimum standards, such as the mandatory use of encryption for PHI, are not established.

There is a further concern raised by our review of the policies and procedures and information gathered at our meetings. We understand that latitude is given to each department to establish its own security practices and standards. In some cases, the onus of ensuring appropriate security measures appears to be placed on individual staff members. Given the importance of the security of PHI, SickKids must ensure that it has a comprehensive corporate policy established and put into place, and that all staff are informed and educated about this policy. In addition, it should not be left to the discretion or judgement of individual staff members to determine how to ensure that appropriate security measures are in place.

This incident is an excellent example of why a comprehensive corporate policy encompassing all departments of a large institution such as SickKids is vital. A staff member demonstrated poor judgement in leaving a laptop computer in a vehicle (despite attempts to conceal it) in a parking lot in downtown Toronto, an area targeted by thieves. That laptop contained identifiable patient information in unencrypted form. A written and enforced corporate policy prohibiting the removal of identifiable patient information from the hospital might have prevented this incident. Similarly, a clear corporate policy requiring the encryption of PHI on desktop and laptop computers would have provided an essential level of protection. Finally, the enabling of all computing devices with the appropriate security protections by the hospital's IT department would not have left this important function to be decided by an individual staff member.

Corporate responsibility for security recognizes that technical safeguards may become outdated over time as technology evolves. Password protection, which is extensively canvassed in SickKids' policies, can no longer be considered to provide adequate security. Password "crackers" are easily available and may well be part of a network administrator's tool kit in order to help staff who have forgotten or lost their passwords. PHI of this very sensitive nature must be either de-identified or encrypted if on disk, e-mailed or stored on a laptop computer.

Encryption is a common and potentially effective mitigation to the risks associated with having PHI accessed outside of normal network protections. Encryption is the practice of encoding a message or data in such a manner as to render it into a meaningless array of letters, numbers and symbols. Such encoding, or encryption, is accomplished by the use of a computer algorithm and encryption keys. If relatively current encryption tools are used, PHI is effectively rendered meaningless. This significantly reduces the risk of a privacy breach to a truly negligible level, provided that the encryption keys are not included with or in the lost or stolen laptop. While encryption may have an impact on system performance, it so clearly addresses the risk of a privacy breach that the onus must be on the organization to justify not using it. For health information custodians, the encryption of PHI on vulnerable computing devices, particularly laptops, should now be viewed as the rule, not the exception.

An alternative to the use of encryption is to refrain from travelling with PHI, leaving it on secure servers, and accessing it remotely through a secure connection or through a VPN. One example of remote access is the Internet itself. Browsers allow access to information on remote

and secure servers, without necessarily having to have a copy of the information on the local computer. Browsers can be set not to retain local copies of the data presented, and web sites can be set to allow only authenticated users to have access. Alternatively, a VPN is a special type of remote access in which a secure connection is made between a remote computer, such as a laptop, and the computer network at the organization's office. This typically requires an internet connection, but does not use a web browser. A VPN allows remote users to access most or all of the features of the organization's network as if they were in the office. While both remote access and VPN's may present different sets of risks, when properly set up, they will reduce or eliminate the privacy impact of having a stolen or lost laptop computer.

SickKids acknowledges that they lacked cohesive hospital-wide, up-to-date policies and practices that set out the specific responsibility and steps required to ensure the security and privacy of PHI stored on laptops. SickKids also acknowledges that, as the health information custodian, it is responsible for ensuring that these policies and practices are in place, across all its departments, including, but not limited to, the corporate, research and IT departments. As noted earlier, SickKids has taken an excellent first step in establishing comprehensive, corporate-wide policies by prohibiting the removal of any identifiable patient information from its premises.

In its written representations, SickKids has advised the IPC that it has initiated a comprehensive review of its current policies and procedures to ensure consistent and mandatory levels of security protection are applied across all departments by clinicians and researchers. In meeting this objective, SickKids' Privacy Committee has devised a hospital-wide "Privacy Improvements Project Plan," which is intended to specifically address the security risks involved with PHI contained on mobile computing devices. This includes the development of three new policies on the topics of security of PHI, removal of identifiable health information and the use and control of laptop computers and portable storage devices. These policies will reflect and incorporate current technological advances available to safeguard PHI, and will be supplemented by a newly devised staff education and training program.

Lastly, SickKids has advised the IPC that it is also working on a project to implement a centrally managed encryption solution that will protect any type of confidential data copied to a mobile computing device.

In summary, based on a review of the policies provided to the IPC, although SickKids is in the process of developing new policies, at the time of this incident, there was no consistent policy in place at SickKids that set out minimum mandatory levels of security and privacy protection, nor a policy that set out how a clinician/researcher could obtain this level of protection. As a result, I am not satisfied that SickKids meets the requirements of section 12(1) of the *Act*.

Section 12(2) of the *Act*

With respect to section 12(2) of the *Act*, I find that there are reasonable grounds to believe that the PHI may have been accessed by unauthorized persons, namely the person(s) who stole the laptop computer and its recipient(s). Although the laptop computer was password protected,

there are products currently available on the market that can "crack" passwords with remarkable speed and ease, making the PHI readily available to the unauthorized user.

I also note that the information on this particular stolen laptop computer is highly sensitive. It consists of PHI, including, in some cases, medical diagnoses. In other cases, the data touches on family members as well. The affected individuals and their family members would clearly be very upset if this PHI fell into the wrong hands.

In meetings with the IPC, SickKids advised the IPC that it agrees that section 12(2) applies in this situation. Given that the majority of affected individuals had transitioned to adulthood and were no longer active patients at SickKids or were deceased, notification was particularly challenging in this case. The contact information for these patients was most likely out of date and any attempt to provide written notification might cause a further privacy breach.

In its written submissions, SickKids indicates that it has demonstrated full compliance with section 12(2) in that:

- SickKids has sent out written letters to active patients with current contact information, notifying them of the breach and providing a contact person should questions arise;
- SickKids is informing active patients whose PHI was of a particularly sensitive nature in person at their next scheduled clinic appointment; and
- SickKids issued a press release on March 1, 2007, which is also posted on its Internet site. The press release provides information about the breach and designates a contact person the public may contact with any inquiries.

Based on the above information provided by SickKids and the particular circumstances of this case, namely, the challenge in notification given the outdated and unreliable patient contact information, and the resulting risk to privacy in attempting to send letters to those addresses, I find that SickKids has complied with the notification requirement of section 12(2) by notifying the active patients individually, either verbally or in writing, and by issuing a press release to the public, and by posting it on its website.

Issue D: Did SickKids, as the health information custodian, comply with section 13(1) of the *Act*?

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

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

SickKids advised the IPC that all of the PHI that was stored on the laptop computer was not permanently lost, as it was also saved on the main server.

Notwithstanding the fact that the PHI was "backed up" on the main server, it cannot be said that the information was retained securely, given the theft of the laptop computer, and the absence of appropriate security measures as noted above.

As discussed in detail under "Issue C" of this document, while many of SickKids' policies refer to the importance of the security of "confidential" information, the policies are inconsistent. They do not clearly set out the specific steps required to ensure that security, and are not in keeping with current technological advances.

In its written submissions, SickKids has advised the IPC that it is exploring alternative safeguards to those presently in place to ensure that its security practices are in keeping with evolving technological advances and current industry standards.

As a result, I find that SickKids, as the health information custodian, did not ensure that the records of PHI in its custody or under its control were retained in a secure manner and, therefore, did not comply with section 13(1) of the *Act*.

Issue E: Did SickKids, as the health information custodian, comply with sections 37(1)(j) and 37(3) of the *Act*?

Section 37(1)(j) of the *Act* provides as follows:

> A health information custodian may use personal health information about an individual,
>
> (j) for research conducted by the custodian, subject to subsection (3), unless another clause of this subsection applies.

Section 37(3) of the *Act* provides as follows:

> Under clause (1)(j), a health information custodian may use personal health information about an individual only if the custodian prepares a research plan and has a research ethics board approve it and for that purpose subsections 44(2) to (4) and clauses 44(6)(a) to (f) apply to the use as if it were a disclosure.

Section 44(1) of the *Act* states, in part:

> A health information custodian may disclose personal health information about an individual to a researcher if the researcher,
>
> (a) submits to the custodian,
>
> (i) an application in writing,
>
> (ii) a research plan that meets the requirements of subsection (2), and
>
> (iii) a copy of the decision of a research ethics board that approves the research plan.

Section 44(2) of the *Act* provides:

> A research plan must be in writing and must set out,
>
> (a) the affiliation of each person involved in the research;
>
> (b) the nature and objectives of the research and the public or scientific benefit of the research that the researcher anticipates; and
>
> (c) all other prescribed matters related to the research.

Section 16 of the regulations of the *Act* states, in part:

> The following are prescribed as additional requirements that must be set out in research plans for the purposes of clause 44(2) of the *Act*:
>
> 4. An explanation as to why the research cannot reasonably be accomplished without the personal health information and, if it is to be linked to other information, an explanation as to why this linkage is required.
>
> 6. A description of the reasonably foreseeable harms and benefits that may arise from the use of the personal health information and how the researchers intend to address those harms.
>
> 8. The safeguards that the researcher will impose to protect the confidentiality and security of the personal health information, including an estimate of how long information will be retained in an identifiable form and why.

Section 44(3) of the *Act* states, in part:

> When deciding whether to approve a research plan that a researcher submits to it, a research ethics board shall consider the matters it considers relevant, including,
>
> (a) whether the objectives of the research can reasonably be accomplished without using the personal health information that is to be disclosed;
>
> (b) whether, at the time the research is conducted, adequate safeguards will be in place to protect the privacy of the individuals whose personal health information is being disclosed and to preserve the confidentiality of this information.

Section 44(6) of the *Act* states, in part:

> A researcher who receives personal health information about an individual from a health information custodian under subsection (1) shall,
>
> (a) comply with the conditions, if any, specified by the research ethics board in respect of the research plan.

SickKids provided the IPC with copies of specific policies and protocols relating to the security of the PHI of research subjects. SickKids also provided copies of its long and short application forms and REB approvals from some of the applicable research studies. SickKids also advised the IPC that it follows the Tri-Council Policy Statement entitled *Ethical Conduct for Research Involving Humans*.

Based on a review of these policies, it is clear that SickKids values the confidentiality of research data as evidenced by the assurances given regarding confidentiality in its research consent forms and in the protocol for researchers on accessing information from health records. In addition, SickKids' REB has a document entitled *"Personal Health Information Privacy Act, 2004 & REB Review of Health Record/Database Research,"* which states that research investigators must sign a data privacy agreement, found in the application form, which sets out the restrictions placed on the investigator for research use of PHI. However, the above documents, including the short and long form applications, do not appear to incorporate the requirements of research plans set out in section 44(2)(c) of the *Act* and section 16 of its regulations.

Both section 44(2) of the *Act* and, in particular, section 16 of the regulations clearly set out the requirements of a research plan, including:

- how PHI will be used;
- an explanation as to why the research cannot reasonably be accomplished without the PHI;
- a description of the reasonably foreseeable harms and benefits that may arise from the use of the PHI; and
- the safeguards that the researcher will impose to protect the confidentiality and security of the PHI, including an estimate of how long information will be retained in identifiable form and why.

SickKids' research applications/plans do not directly address the above requirements, and refer only to the use of de-identification, password protection and limiting access as optional and potentially mutually exclusive safeguards.

In Ontario, there are human subject research applications available that comply with the requirements set out the *Act*. For example, the Toronto Academic Health Sciences Network (TAHSN) human subjects research application contains a comprehensive and detailed section relating to privacy and confidentiality of PHI used in research. The applicant must, among other things:

- describe the safeguards that will be put in place to protect the confidentiality and security of research data;
- indicate how long the PHI will remain identifiable and why;
- explain why the research cannot reasonably be accomplished without using PHI;

- describe any harms or benefits that could arise if PHI was inappropriately released and how any consequences would be addressed; and
- describe how and when the PHI will be disposed of or returned to the health information custodian.

I am advised by SickKids that it was involved in the development of the TAHSN application form, but decided against adopting it for its own use due to perceived deficiencies in other aspects of the application. In hindsight, it is unfortunate that SickKids did not adopt the excellent section of the TAHSN application form relating to the privacy and confidentiality of PHI, as it would have encouraged SickKids to turn its mind to these important issues.

Although SickKids advised the IPC that, since the enactment of the *Act*, all research data was required to be de-identified by the researcher, it should be noted that the REB approvals do not stipulate this condition. In fact, the REB approvals do not reflect whether the REB considered the factors required as set out in section 44(3) of the *Act*, including the assessment of safeguards to protect the privacy of research subjects. Similarly, if the REB mandated the de-identification of data, the researcher in this case failed to comply with his responsibilities as set out in section 44(6)(a) of the *Act*.

The Canadian Institutes of Health Research (CIHR) published a very useful and important paper in September, 2005 entitled *"CIHR Best Practices for Protecting Privacy in Health Research."* This paper expands on many of the principles set out in the Tri-Council Policy Statement, which SickKids has indicated it follows. The CIHR best practices stress the importance of organizations ensuring that appropriate organizational security safeguards are in place where research data are held. Researchers should take a risk assessment and management approach to protecting research data from loss, corruption, theft or unauthorized disclosure, as appropriate for the sensitivity and identifiability of the data. After assessing the risk to research data, safeguards should be implemented, updated and regularly reviewed. Some of the technological safeguards that the CIHR recommends are:

- the development, monitoring and enforcement of privacy and security policies and procedures;
- encryption, scrambling of data and other methods of reducing the identifiability of data;
- direct identifiers should be removed or destroyed at the earliest possible opportunity;
- if direct identifiers must be retained, they should be isolated on a separate dedicated server/network without external access;
- special protection for remote electronic access to data should be installed; and
- a detailed audit trail monitoring system should be instituted to document the person, time, and nature of data access, with flags for aberrant use and "abort" algorithms to end questionable or inappropriate access.

Had SickKids adopted and implemented the above-referenced best practices, this incident may have been easily avoided.

In its written submissions, SickKids acknowledged that it needs to update and revise its existing polices relating to research to comply with all of the research provisions found in the *Act*. SickKids has advised the IPC that it is adopting and enhancing the research application forms developed by TAHSN as part of the REB approval process in order to comply with all of the research requirements outlined in the *Act* and the guidelines contained in the Tri-Council Policy Statement entitled *Ethical Conduct for Research Involving Humans*.

Lastly, I must reiterate that it is the health information custodian's overarching responsibility to ensure that PHI used for research purposes is strongly safeguarded. As such, the health information custodian must ensure that it has measures in place that comply with the *Act*, and that the REBs it has established and the researchers, conduct themselves in accordance with the requirements set out in the *Act*.

Therefore, based on information provided by SickKids, I find that SickKids did not comply with sections 37(1)(j) and 37(3) of the *Act* relating to the use of PHI for research purposes as the research plans and REB approvals did not meet the requirements set out in the *Act*.

Issue F: Did SickKids, as the health information custodian, comply with section 10(1) of the *Act*?

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

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

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."

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.

As previously discussed, SickKids has general policies that relate to the privacy and confidentiality of information. However, I note that both policies were last reviewed in 2003, prior to the *Act* coming into force on November 1, 2004. In particular, the privacy policy relates only to "personal information," and makes no reference to PHI as defined in the *Act* and, indeed, makes no reference to the *Act*.

SickKids also has policies entitled *Computer Information Security*, last reviewed in 2003, and *KIDNET (Sick Kids Computer Network) Acceptable Use Policy*, which also make no reference to the *Act* and its requirements to safeguard PHI. In addition, as already noted, the policies do not provide sufficient information to assist a staff member who uses a laptop computer in ensuring the security of PHI. As well, the policies do not reflect and incorporate the current technological advances that are readily available to safeguard PHI, such as the use of encryption software on laptop computers and the use of secure virtual private networks for remote access to information as an alternative to removing identifiable health information from hospital premises. It is my understanding that SickKids is now in the process of developing a policy relating to remote access.

To its credit, SickKids has developed policies that incorporate many of the provisions under the *Act*. For example, there is a policy relating to the disclosure of PHI as permitted under the *Act*. In addition, another policy sets out how the "lockbox" provisions of the *Act* are to be implemented. These policies are a first step in ensuring that information practices are in place that comply with the *Act*.

Lastly, SickKids is currently relying on a critical incident policy in managing this incident, in the absence of a tailor-made, privacy breach protocol/policy. My review of the critical incident policy indicates that it is not suitable for responding to this type of incident or other types of privacy breaches experienced by hospitals. Given the importance of privacy and security of PHI, it is imperative that SickKids develop and put in place a privacy breach protocol/policy to manage similar situations in the future.

In its written submissions, SickKids acknowledged that it needs to adapt and revise its existing information practices to fully comply with section 10(1) of the *Act*. All policies dealing specifically with PHI will include a reference to the *Act* and precise definitions of specific terms to accurately reflect the current wording used in the *Act*. In addition, SickKids intends to amend its MCO policy to include specific considerations for managing privacy breaches. Lastly, SickKids has advised the IPC that it will ensure that its amended information practices, once complete, are clearly and consistently communicated to its leadership team and staff on a go-forward and continuing basis.

Based on a review of SickKids' privacy, technology and research policies and procedures, it is clear that many of the requirements under the *Act* relating to the retention and security of PHI and to its use in research are missing from current policies across many departments. It would

appear that SickKids did not undertake a comprehensive review of their policies when the *Act* came into force on November 1, 2004.

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

In addition, 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.

SUMMARY OF FINDINGS

I have made the following findings in this review:

1. The records at issue are records of "personal health information" as defined in sections 2 and 4 of the *Act*.
2. SickKids is a "health information custodian" (Custodian) as defined in section 3(1) of the *Act*.
3. SickKids, as the health information custodian, did not comply with section 12(1) of the *Act* in that the Custodian did not take steps that were reasonable in the circumstances to ensure that PHI in its custody or control was protected against theft, loss and unauthorized use or disclosure.
4. SickKids, as the health information custodian, is required to notify the individuals whose PHI was contained on the laptop computer pursuant to section 12(2) of the *Act* and SickKids has complied with this notification requirement.
5. SickKids, as the health information custodian, did not comply with section 13(1) of the *Act* in that the Custodian did not ensure that the records of PHI in its custody or under its control were retained, transferred or disposed of in a secure manner.
6. SickKids, as the health information custodian, did not comply with sections 37(1)(j) and 37(3) of the *Act* in that the Custodian used PHI for research not in compliance with the *Act*.
7. SickKids, as the health information custodian, did not comply with section 10(1) of the *Act* in that the Custodian did not have information practices in place that comply with the requirements of the *Act*.

ORDER

1. I order SickKids to develop or revise and implement policies and procedures to ensure that records of PHI are safeguarded at all times as required pursuant to sections 12(1) and 13(1) of the *Act* and that its information practices comply with and incorporate the requirements of the *Act* and its regulations, specifically:

    - a comprehensive corporate policy that, to the extent possible and without hindering the provision of health care, prohibits the removal of identifiable PHI in any form from the hospital premises. To the extent that PHI in identifiable form must be removed in electronic form, it must be encrypted;

    - a hospital-wide endpoint electronic devices policy, applicable to both desktop and portable devices (laptops, PDA's), which mandates that any PHI not stored on secure servers must either be de-identified or encrypted. The policy must also designate the Information Technology department as the centre of responsibility for ensuring that the appropriate software is installed on endpoint electronic devices and that the end user has been provided with sufficient training on its use;

    - a comprehensive corporate policy relating to the use of secure remote access and/or Virtual Private Networks as an alternative to using laptop computers;

    - a privacy breach protocol/policy; and

    - 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, once complete.

2. I order SickKids to review and revise its research protocols and applications to comply with sections 37(1)(j) and 37(3) of the *Act*.

3. In order to verify compliance with this Order, I require that SickKids provide me with proof of compliance, or an update on compliance activities, by June 15, 2007.

COMMISSIONER'S MESSAGE

Mobile computing devices, including laptop computers, flash drives and PDAs are widely deployed in the health care sector in Ontario. Such devices can provide enhanced capabilities for health care providers and enhanced services for patients. But such benefits may also come at a price. The risk of theft or loss of mobile computing devices is known to be high. While laptop computers are often stolen for the value of these devices, in some cases, thieves are becoming increasingly interested in the personal information that they contain. There is no way of distinguishing one kind of theft from another. Personal information stored on stolen devices can be used for purposes such as fraud and identity theft – problems that have reached epidemic proportions throughout North America. And with the movement of organized crime into this area, the problem takes on a greater and more sinister complexion.

In the present incident, while the stolen laptop happened to contain PHI that was being used for research purposes, it could have contained PHI that was being used for any purpose, either inside or outside of the health care facility. Therefore, all health information custodians using mobile computing devices to store PHI can learn from this unfortunate, but predictable, incident.

Health information custodians are required under the *Act* to take steps that are reasonable in the circumstances to ensure the PHI is protected against theft, loss and unauthorized use or disclosure. Accordingly, it is my view that it is no longer reasonable to store PHI on mobile computing devices, unless steps are taken to ensure that any PHI stored on such devices is protected against unauthorized access, in the event that the device is lost or stolen. A multi-layered approach is needed to guard against unauthorized access.

As a first line of defence against unauthorized access, custodians should avoid storing identifiable PHI on mobile computing devices. However, where PHI 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, whenever possible, PHI should be de-identified or coded, in a manner such that the identities of the individuals whose PHI 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 more secure computing device, such as a central server in a health care facility.

Another layer of defence against unauthorized access is the use of password protection. In many circumstances, this is not sufficient, as in this case. Strong passwords consist of at least eight characters and combine letters, numbers and symbols in what appear to be random strings. However, because passwords may be guessed, written down, stolen, shared, hacked or cracked with software that is readily available, they are often the weakest link in the security chain. Consequently, it is my view that password protection alone can no longer be considered to provide adequate protection against unauthorized access to PHI stored on mobile computing devices.

Where identifiable PHI is stored on vulnerable devices, such as laptop computers or flash drives, my position is that the information must be encrypted. At a minimum, files or folders containing PHI should be encrypted. It is essential to use up-to-date encryption techniques to ensure that personal information is appropriately secured. If the chosen encryption technology or software requires a password as a key, then strong passwords, as described above, should be used. The encryption of files and folders should not rely on a user's login password due to the above-noted vulnerabilities associated with such passwords. Similarly, users should know not to use login passwords as passwords to decrypt files and folders. Custodians should look for encryption software packages that have built-in mechanisms to enforce the use of strong encryption keys.

In addition to the encryption of individual files or folders using strong encryption keys, it is also possible to encrypt an entire hard disk within a laptop computer. Full disk encryption is a type of software or hardware that can be used to protect all the data on a hard disk, including the operating system, resident data, temporary files, and deleted files. Other disk encryption software can be used to protect everything on a hard disk, except the operating system.

The importance of information security has been carefully considered by the state of California, which has taken the lead with many privacy and data security issues. In 2002, California enacted breach notification legislation that requires all organizations to notify California residents when their unencrypted, computerized personal information is, or is reasonably believed to have been, acquired by an unauthorized person. Given that no company wants to tell customers that its systems were, for example, "hacked" and sensitive data was accessed, the potential effect of this law's mandatory notification highlights the advantages to encrypting information as a means of avoiding embarrassing privacy breach incidents.

Consequently, to the extent that personal health information on a mobile computing device has been encrypted to protect it from unauthorized access, I would not consider the theft or loss of that device to be a loss or theft of PHI. The *Act* requires custodians to notify an individual at the first reasonable opportunity if PHI is stolen, lost or accessed by unauthorized persons. If the case can be made that the PHI was not stolen, lost or accessed by unauthorized persons as a result of the loss or theft of a mobile computing device because the data were encrypted (and encrypted data does not relate to identifiable individuals), the custodian would not be required to notify individuals under the *Act*.

I would also like to advise health information custodians that there is an emerging focus on data security and information breaches, not only in the United States, but also in Europe. Recently in the United Kingdom, its financial services regulator levied a substantial fine against a building society, following the theft of an employee's laptop that contained personal information relating to approximately 11 million customers. In addition to being fined, the organization was heavily criticized for failing to adequately address the risk that customer data might be lost or stolen and for having inadequate security procedures. This case illustrates the importance of the security of personal information, and the lessons learned may easily be applied in the health sector.

Therefore, I strongly urge all health information custodians to regularly review their privacy and security policies and procedures relating to the storage of PHI on mobile computing devices to ensure that they are effective in minimizing the significant risk to privacy posed by the loss or theft of such devices. All custodians should invest in proactive measures to protect PHI stored on mobile computing devices. In the event that a mobile computer device is lost or stolen, this would save custodians time and money by allowing them to avoid the notification requirements of the *Act*, and prevent the potentially irreparable damage to a custodian's reputation resulting from the loss or theft of PHI. More importantly, it would protect individuals from the undue stress of knowing that their PHI had been lost or stolen.

There is no excuse for unauthorized access to personal health information due to the theft or loss of a mobile computing device – any PHI contained therein must be encrypted.

March 7, 2007

Ann Cavoukian, Ph.D.
Commissioner

Date