Medical records and encryption
Sensitive information on laptops and other mobile computing devices must be protected, says Ontario Privacy Commissioner

Introduction
There are many rules pertaining to medical records including regulations made under the Medicine Act, obligations that arise under the Public Hospitals Act, the Long-Term Care Act, the Personal Health Information Protection Act and expectations set out in the College’s Medical Records policy. Physicians need to be aware that they have obligations to keep medical records secured and that good record keeping is a crucial part of providing the best quality of medical care.

IPC Fact Sheet
In May 2007, the Information and Privacy Commissioner’s office released a fact sheet on encryption that is intended to assist health information custodians who store personal health information on mobile computing devices.

The fact sheet explains the difference between strong and weak passwords, defines encryption and its types, and sets out encryption standards. It also provides an encryption checklist along with a sample of several encryption solutions currently available.

In this fact sheet, the Commissioner promotes the use of encryption as the most effective technology for preventing the disclosure of patients’ personal health information stored on mobile devices.

The fact sheet is available at: www.ipc.on.ca.

In addition, to provide patients with the best care possible, physicians need to be able to use and share patient information freely and rapidly. Technology which allows for a shift from paper-based records to electronic ones can greatly enhance communications, thus improving patients’ safety to the benefit of both patients and physicians. Therefore, the College supports the significant role that information technology is assuming in the health-care system.

However, as physicians come to rely on mobile computing devices – such as laptop computers, personal digital assistants and flash drives – to hold patient health information, new risks about security arise. The high incidence of loss or theft of these devices requires physicians to ensure that personal health information stored on such devices is adequately secured.

This article is intended to remind physicians of existing rules relating to medical records as well as to present advice on the protection of electronic records provided by the Privacy Commissioner, Dr. Ann Cavoukian, in her recent Order.

Medical Records Policy
The College’s Medical Records policy states that physicians must take reasonable steps to ensure that records are protected from theft, loss and unauthorized use or disclosure, including photocopying, modification or disposal.

What is reasonable depends on the threats, risks and vulnerabilities to which the information is exposed, the sensitivity of the information, and the extent to which it can be linked to an identifiable individual. Consideration must be given to each of the following aspects of record protection:

• Physical security (locked file cabinets, restricted office access, alarm systems).
• Technological security (passwords, encryption and firewalls).
• Administrative controls (security clearances, access restrictions, staff training, and confidentiality agreements).

Personal Health Information Protection Act (PHIPA)
Personal health information in Ontario is protected under the Personal Health Information Protection Act, 2004 (PHIPA). As health information custodians, physicians are also governed by PHIPA. The Act requires all health information custodians to take reasonable steps to ensure information is protected against theft, loss and unauthorized use or access. However, the meaning of reasonable steps has changed along with the technological change that requires more sophisticated safeguards in order to protect personal health information.
The Commissioner oversees *PHIPA*. Recently, the Commissioner issued her 4th Order under the Act. This is in regard to a privacy breach at the Hospital for Sick Children (HSC) in Toronto.

In that Order, the Commissioner provided some useful guidance for all Ontario physicians with respect to fulfilling their obligations under *PHIPA* and safeguarding personal health information in their custody or control.

The Order was issued on March 8, 2007, following the off-site theft of a laptop computer which belonged to HSC.

A physician, who is also a researcher at HSC, took a laptop from his office with the intention of analyzing some research data at home. On the way home, he ran an errand. He parked his minivan, hid the laptop from view (there was no trunk), and locked the vehicle. Upon his quick return to the minivan, he noticed that his passenger window had been broken and that the laptop was stolen.

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.

The personal health information stored on the stolen laptop included patients’ names and individual HSC numbers, as well as information relating to the patients’ medical conditions. In some cases, very sensitive information was also included, such as drug therapy and HIV status.

The laptop was password protected, but personal health information that it contained was not encrypted.

While laptop computers are often stolen simply for the value of these devices, in some cases, thieves are interested in the personal information that they contain. There is no way of distinguishing one kind of theft from another. Therefore, the Commissioner decided that individuals affected by the HSC breach must be notified even though there was no evidence that the thief was after the information rather than the laptop.

Many people would view the steps that the physician took – hiding the laptop from sight and locking the vehicle – as reasonable measures. Similarly, protecting a computer with a password would also be viewed by many as a reasonable measure.

However, the Commissioner argued that these measures are insufficient in the current environment. She noted that although the information on the laptop was password protected, there are products currently available on the market that can “crack” passwords with remarkable speed and ease, making the personal health information readily available to the unauthorized user. Accordingly, the Commissioner has said that, in her view, it is no longer reasonable to store personal health information on mobile computing devices, unless steps are taken to ensure that any personal health information stored on such devices is protected against unauthorized access, in the event that the device is lost or stolen.

The College recognizes that encryption may not be a simple process. Physicians may well be unfamiliar with the encryption software or have difficulty implementing it. However, the Commissioner has made it clear that she considers encryption of personal health information on mobile computing devices to be the rule, not the exception. Therefore, it is in the physicians’ best interests to consider this option in their practice.

If properly implemented, encryption would prevent a privacy breach in the event that a mobile computing device (e.g., laptop) containing personal health information is lost or stolen. This would save physicians time and money by allowing them to avoid the notification requirements of *PHIPA*. It would also protect individuals from the stress of knowing that their personal health information is not adequately protected.
In early June, Ontario’s Information and Privacy Commissioner, Dr. Ann Cavoukian, issued an Order urging all physicians to immediately review any wireless communication technologies they are using and to take reasonable steps to minimize the privacy risks posed by such technologies.

The Order, which comes under the Personal Health Information Protection Act, follows the Commissioner’s investigation into the use of a wireless video camera at a methadone clinic for the purpose of monitoring sample collection for urine drug testing. Commissioner Cavoukian found that the methadone clinic had been completely unaware that its video images could be intercepted – in this case by a “back up” camera in a vehicle parked near the clinic.

When the clinic became aware of the privacy breach, it immediately turned off the wireless video camera and replaced it with hardwired technology; notified patients of the breach; and notified the College to alert other methadone treatment practitioners that wireless camera systems are not secure and pose significant risks to patients’ privacy.

The College has sent a communiqué regarding the risks of using wireless technologies to all methadone practitioners and highlighted this issue in the June edition of the Methadone Newsletter.

In addition, the messages in the Commissioner’s Order are reinforced with a fact sheet entitled, Wireless Communications Technologies: Video Surveillance Systems, which highlights the need for physicians to protect personal information collected by wireless communication technology.

The IPC Order and fact sheet are available at: http://www.ipc.on.ca/images/Findings/up-ho_004.pdf

What is Next?
The College reminds physicians that they are responsible to ensure that personal health information in their custody or control is appropriately secured. Accordingly, it is imperative that strong, preventive safeguards be used. Implemented properly, encryption fulfills this requirement and, as such, is in the physicians’ best interests.

However, the College also recognizes that encryption is a complex process.

As this is a changing environment, the College will continue to work on these issues and will be providing you with updates, as necessary. The College also welcomes any comments that you may have on the issue of encryption.

The IPC Order is available at: http://www.ipc.on.ca/images/Findings/up-ho_004.pdf

Methadone clinic’s video images intercepted

In early June, Ontario’s Information and Privacy Commissioner, Dr. Ann Cavoukian, issued an Order urging all physicians to immediately review any wireless communication technologies they are using and to take reasonable steps to minimize the privacy risks posed by such technologies.

The Order, which comes under the Personal Health Information Protection Act, follows the Commissioner’s investigation into the use of a wireless video camera at a methadone clinic for the purpose of monitoring sample collection for urine drug testing. Commissioner Cavoukian found that the methadone clinic had been completely unaware that its video images could be intercepted – in this case by a “back up” camera in a vehicle parked near the clinic.

When the clinic became aware of the privacy breach, it immediately turned off the wireless video camera and replaced it with hardwired technology; notified patients of the breach; and notified the College to alert other methadone treatment practitioners that wireless camera systems are not secure and pose significant risks to patients’ privacy.

The College has sent a communiqué regarding the risks of using wireless technologies to all methadone practitioners and highlighted this issue in the June edition of the Methadone Newsletter.

In addition, the messages in the Commissioner’s Order are reinforced with a fact sheet entitled, Wireless Communications Technologies: Video Surveillance Systems, which highlights the need for physicians to protect personal information collected by wireless communication technology.

The IPC Order and fact sheet are available at: www.ipc.on.ca.

A second IPC fact sheet covering the broader range of wireless communication technologies is forthcoming. The College will continue bringing you updates on this issue, as necessary.