Information and Privacy Commissioner/ Ontario

ORDER HO-005

Ann Cavoukian, Ph.D.
Commissioner
June 2007

BACKGROUND

On April 30, 2007, the Office of the Information and Privacy Commissioner/Ontario (IPC) was contacted regarding a media report that a video image of a patient attending a methadone clinic (the Clinic) had been accessed by a wireless mobile rear-assist parking device ("back up camera") in a car parked near the Clinic. The Clinic is located at 310 Larch Street, Sudbury, Ontario, and is owned and operated by Brian Dressler Medicine Professional Corporation. The IPC immediately commenced an investigation of this incident, pursuant to the *Personal Health Information Protection Act* (the *Act*).

NATURE OF THE INCIDENT

A reporter from the Canadian Broadcasting Corporation (the CBC) advised the IPC that she had been notified by an individual who, much to his surprise, had viewed an image of a toilet in a washroom on his vehicle's back up camera, while driving by the Clinic.

The reporter also advised the IPC that, after receiving the above information from the individual, she contacted a private investigator to seek his assistance in determining if what she had been told was indeed possible. The reporter and the private investigator subsequently drove by and stopped at the Clinic in a vehicle that had a back up camera installed in it. Back up cameras are being used with more frequency to assist drivers in reversing their vehicles safely. The reporter and the private investigator then saw, on the back up camera's monitor, a disturbing image of a woman using a toilet. It is my understanding that the image of the woman included a reasonably detailed image of her face.

As a result of seeing the image, the reporter recognized and spoke to the woman as she left the building. The woman indicated that the Clinic was a methadone clinic, and that she was aware of the presence of a surveillance camera in the washroom. She indicated that patients of the Clinic are monitored while providing urine samples to ensure that the samples are not tampered with. In addition, she advised the reporter that her written consent had been sought and provided to the Clinic to engage in this practice.

Upon notification of the incident by the CBC, the IPC contacted the Clinic right away to investigate this matter. The IPC advised them of the two incidents and asked the Clinic to immediately turn off the camera and contact the security firm to ensure that this type of incident could not occur again in the future. The Clinic complied with the IPC's requests without any delay and, the next day, replaced its system, which had operated using wireless technology, with one that is now wired.

CONDUCT OF THE REVIEW

As indicated, the IPC was initially advised of the incident by the CBC. Further information was provided by the Clinic to the IPC during telephone interviews with my staff and by way of written submissions dated May 25, 2007, in response to the IPC's notice of review and request for submissions, including the following:

The Clinic advised the IPC that it monitors patients providing urine samples to ensure that the samples provided for drug testing emanate from the correct source and are not tampered with. The Clinic advised the IPC that this practice is in accordance with the *Methadone Maintenance Guidelines* (Guidelines) published by the College of Physicians and Surgeons of Ontario (the CPSO) in November, 2005. The Clinic also advised that the CPSO provided further direction to methadone clinics by way of a newsletter entitled *Methadone Program Newsletter*, dated June 2006, that the supervision of patients providing urine samples should be observed in real time and the use of video recording equipment for urine screening was not acceptable.

In addition, the Clinic advised the IPC that its patients provide informed consent by entering into a written agreement with the Clinic, in which the patient agrees to provide supervised urine samples for drug screening purposes. The Clinic provided a sample copy of the agreement it uses, entitled *Methadone Agreement*, to the IPC. The IPC reviewed the Clinic's agreement and was satisfied that it conformed with the CPSO's Guidelines, which permit the taking of supervised urine samples for drug screening purposes. The Clinic's contract was in fact essentially the same as the sample contract contained in the CPSO's Guidelines.

When patients provide a urine sample at the Clinic, a notation is made next to the patient's name on a form indicating that a urine sample had been properly provided, and on a given date. If tampering of the sample is suspected, a separate notation is made in the patient's health record.

It is my understanding that the Clinic asked the Sudbury Police to recommend a security firm for the purpose of installing a burglar alarm system (not a video surveillance system). The police recommended a particular security firm as being reputable and experienced. The Clinic retained the security firm. While the burglar alarm system was being installed, the Clinic made inquiries of the security firm's technician regarding the installation of a video camera system. As a result, the security firm recommended and installed three 2.4 Ghz frequency wireless camera/receiver kits. There is no written work order or contract for the installation of the wireless camera system, as the Clinic verbally approved the system.

The three wireless cameras' receivers were directly connected to a single monitor, with no recording device attached. According to the Clinic, the system was designed so that the images could only be monitored in real time by Clinic staff in the nurse's observation station. In addition, the system was not connected to a computer or the Internet.

Regarding the incident itself, the Clinic learned of it for the first time when notified by the IPC. The same day that we advised the Clinic of the incident, it contacted its security firm, and a

technician was dispatched to the Clinic that very day. The technician advised the Clinic that its surveillance cameras operated on wireless technology, and, as a result, the images in the camera could be viewed on any other wireless device that utilized the same frequency. It appears that the Clinic was unaware of the fact that the security firm had installed a wireless system. The Clinic also advised the IPC that it was completely unaware of the possibility that any interception of the washroom's video images could take place.

The technician immediately made arrangements to rectify the situation and the next day replaced the system, including the wireless cameras and receiver, with a set of regular (non-wireless) closed circuit television cameras (CCTV[1]) that are wired directly to the nurse's observation station. Thus, there is no longer a wireless signal being broadcast.

At the Clinic's request, the security firm also conducted a security review of the new wired system and has confirmed, in writing, that it is a secure system.

In addition, the Clinic notified the CPSO of the incident and asked the CPSO to advise other methadone clinics in Ontario that video surveillance cameras should not operate on unsecured wireless technology. As a result, the CPSO issued a communication entitled *Communiqué to Methadone Prescribers*, on May 15, 2007, directing methadone prescribers to:

> …immediately disconnect any wireless camera systems that you are using for the purpose of urine collection.

The IPC also contacted the CPSO to confirm that it had been advised of the incident, and to urge the CPSO to contact other methadone clinics in Ontario to alert them to the fact that wireless technology, in and of itself, is not secure. The CPSO verified that it had been advised of the incident, and had sent out the above described direction to methadone prescribers, which included the following statement:

> …the use of wireless camera systems is not secure, [and] can be easily compromised, thereby jeopardizing patients' privacy.

The Clinic also worked with the IPC in drafting a notice regarding the incident. The notice is currently posted in the Clinic, advising all patients of the incident and the steps taken by the Clinic to prevent this type of situation from ever arising.

I would like to acknowledge the full cooperation given to my staff by the Clinic during the course of this investigation. Staff of the Clinic was at all times fully engaged in ensuring that a comprehensive investigation was completed and that swift and meaningful measures were put into place to lower the risk of a reoccurrence of this type. I applaud the Clinic for acting quickly to address this issue and for proactively contacting the CPSO to alert other clinics.

1 CCTV is an acronym for Closed Circuit Television. The term originally applied to a system consisting of a video camera attached to a video screen using NTSC/PAL video timing that typically was used for building or site security. The term has become a generic reference to any system enabling remote viewing of video images and is being used in that sense here.

ISSUES ARISING FROM THE REVIEW

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

(A) Is the information at issue a "record" of "personal health information" and is it in "recorded form" under sections 2 and 4 of the *Act*?

(B) Is Brian Dressler Medicine Professional Corporation a "health information custodian" as defined in section 3(1) of the *Act*?

(C) Did the Custodian comply with sections 12(1) and (2) of the *Act*?

RESULTS OF THE INVESTIGATION

Issue A: Is the information at issue a "record" of "personal health information" and is it in "recorded form" under sections 2 and 4 of the *Act*?

Introduction

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

> 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* reads, in part, as follows:

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

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

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

"Record" and "recorded form" under sections 2, 4(1)

The Clinic submits that the image in question does not constitute personal health information, because the surveillance system did not record any audio or video images. Specifically, the Clinic states:

> . . . The images that were viewed were, in accordance with CPSO policy, live images. As such, the viewing is analogous to a third party looking into a window of the Clinic . . .
>
> . . . The mere fact that an image may have been capable of being recorded is not sufficient . . .
>
> Furthermore, a "record" is a distinct, defined term in [the *Act*] and the subject of specific requirements (see *e.g.* section 13 and Part V re: access and correction rights). We are not aware of any provision in the Act, or the regulations, that would extend the definition of "a record" to include an image that merely is capable of being recorded. Returning to our analogy of the client being viewed through a washroom window, a voyeur with a camera is capable of "recording an image" but this would not constitute a record of personal health information in the custody or control of a health information custodian.
>
> . . . [Section] 7 illuminates the objects and focus of the Act – the collection and disclosure of personal health information. The Act does not deal broadly with the subject matter of privacy in health-related matters. Rather, the specific focus is on the storage and dissemination of health information. It is important to emphasize that at no point has there been any allegation that actual patient records have been lost, stolen, accessed or improperly disclosed.

I do not accept the Clinic's submissions on this point. I find that the Clinic created a record when its camera and transmitter captured an image of a woman using the washroom, and then encoded and wirelessly transmitted that image. This meets the definition of "record" under section 2 of the *Act*.

While the word "record" may be viewed narrowly as having a high degree of permanence, it may also be viewed broadly. For example, the definition of "record" in the *Canadian Oxford Dictionary* includes the following:

> **1a** a piece of evidence or information constituting an (esp. official) account of something that has occurred, been said, etc. (p. 1206)

In addition, I note that in the United States, the *Uniform Electronic Transactions Act*[2] defines "electronic record" as:

> …a record created, generated, sent, communicated, received, or stored by electronic means.

2 The *Uniform Electronic Transactions Act* was completed by the Uniform Law Commissioners in 1999, was approved by the American Bar Association, and has been adopted by 46 states – see http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-ueta.asp.

In my view, the broad interpretation of "record" is preferable in this context, since it promotes the fundamental health privacy purpose of the *Act* as set out in section 1(a). If I were to find otherwise, a modern technology, in the form of wireless communication, which is widely used to communicate personal information (and is becoming more and more prevalent) may not be covered by the *Act*, simply on the basis that the images are not recorded in the traditional sense.

It might be argued that the Legislature could not have intended to capture information that may be incapable of being used or retrieved after it is created. I do not accept this argument, mainly because it conflicts with the fact that in the section 4(1) definition of "personal health information," the Legislature included "oral" information, a type of information that, as in this case, lacks permanence and may not be capable of being used or retrieved after creation.

In the present case, at the time that the Clinic broadcast the video image, a "record" was created in the sense of an account of something that occurred (see *Oxford Dictionary* definition above), specifically, a woman using the washroom to provide a urine sample. That record was created electronically in the form of encoded data. The wireless transmission of this data is analogous to a conversation, in which sound is "encoded" with information through the use of language. A wireless broadcast also encodes its transmission with information, in this case, the image of a person using a washroom. Once the wireless signal containing the data has been emitted, it cannot be called back, and continues indefinitely, carrying with it the personal information (video image) with which it was encoded. Like a conversation, it may be "overheard" by anyone with an "ear" to hear it – in this case, a wireless receiver in a passing car. While the Clinic did not retain the image in a manner capable of later being used, it could nonetheless be used by others who intercepted the wireless signal and who may have retained it. Even if the image was not intercepted, it became a record upon being converted to data.

Further, I find that when the CCTV camera captured the image of the woman, the Clinic created information in "recorded form" under section 4(1) of the *Act*, for essentially the same reasons set out above.

In the past, the act of creating a record was a physical act that created a physical artefact such as a written or printed page. Such records could be stored and retrieved in a variety of ways. This form of record storage is becoming a less common way of storing and retrieving information. The distinction between "data" and "records" is becoming increasingly more difficult to discern, and thus, of limited use. *Digital data are indeed records in any meaningful way*. When information is digitized, whether by scanning a piece of paper, typing onto a word processor, or by capturing a video image, that information is "encoded" onto some form of medium in a way that is analogous to writing onto paper. The difference is that the medium is not necessarily transformed in a visible or immediately perceptible manner.

Digitizing information to create data creates a digital artefact on a medium. The artefact may be a specific arrangement of magnetic charges on a hard drive, a series of microscopic imperfections on a compact disc, specific modifications to a radio signal, or a particular arrangement of signals to an LED screen. The characteristic of such digitized information that makes it useful as a

method of recording information is persistence – whether for decades in the case of compact discs, or for the microseconds it takes a weak wireless broadcast to dissipate into meaningless noise. One aspect of encoding data to a medium is that it may be read by an individual, or read by a device such as the system that created it (and then viewed by an individual). The latter is what happened in this case.

The Clinic submits that when the surveillance system captured the images, this was analogous to a third party looking into a window at the Clinic. This analogy does not hold true. In the case of a person looking into a window, the Clinic would not have created a record of what was occurring in any form, electronic or otherwise, and thus the definition of "record" would not apply. Further, if that outside person were to record what he or she saw, the definition of "record" still would not be met since, again, the Clinic would not have created a record in any form. Therefore, contrary to the Clinic's submissions, I am not finding that the information in question constitutes a record merely because it is "capable of being recorded." My finding is based on the fact that the Clinic's surveillance system did indeed create an electronic record.

It may also be argued that the broadcast video images are akin to an "oral form" of information under section 4(1) of the *Act*, in the sense that oral refers to information conveyed through the air by sound waves and frequencies. Similarly, images captured by wireless technology are transmitted through the air by radio waves at various frequencies. In this sense, wireless communication directly parallels oral communication.

The Clinic also retained written records indicating that certain individuals were patients at the Clinic and had provided urine samples, on particular dates. The wireless video image indirectly disclosed these facts, contained in the Clinic's written records, with respect to the woman whose image was broadcast (see, for example, IPC Investigation Reports MC-980055-1 and PC-060004-1).

Accordingly, I find that the video image in this case constitutes a "record" under section 2 of the *Act*. I also find that this information is in "recorded form" under section 4(1) of the *Act*.

In addition, I find that the Clinic's written records indicating that certain individuals were patients at the Clinic and had provided urine samples on particular dates falls within the definition of "personal health information" that is in recorded form under sections 2 and 4 of the *Act*.

"Identifying information" under sections 4(1) and (2)

As indicated above, the video image in question included depictions of the face of the individual. In these circumstances, it is my view that it is reasonably foreseeable that any person in the vicinity of the Clinic who received and viewed the video images could use the information to identify that individual (as did the CBC reporter). This view is consistent with decisions of my office under the *Freedom of Information and Protection Privacy Act* that deal with the issue of whether individuals are considered to be "identifiable" from images (for example, Order PO-2477). Therefore, the video image qualifies as "identifying information" under sections 4(1) and (2) of the *Act*.

"Personal health information" under sections 4(1)(a) and (b)

As indicated above, the broadcast video image revealed the fact that a woman had used the washroom in the Clinic and provided a urine sample. More particularly, the image allowed for the disclosure that the woman was a patient and was receiving methadone-related services at the Clinic. These facts constitute identifying information about the woman that relates to her physical or mental health under section 4(1)(a), and relates to the provision of health care to her under section 4(1)(b) of the *Act*.

In any event, I cannot imagine any circumstance where it would be acceptable for a health information custodian (custodian) to allow video images of its clientele using washroom facilities to be broadcast to the general public. Such a scenario is obviously not in keeping with the purpose or the spirit of the *Act*, and was immediately recognized by the Clinic as clearly unacceptable. Similarly, the transmission of images of a patient in the act of providing a urine sample is far more intrusive and devastating to the patient than having the paper records related to that sample fall into the wrong hands.

Accordingly, the video image qualifies as "personal health information" under sections 4(1)(a) and (b) of the *Act*.

To conclude Issue A, the video image is a "record" of "personal health information" and is in "recorded form" under sections 2 and 4 of the *Act*.

Issue B: Is Brian Dressler Medicine Professional Corporation 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:
>
> 1. A health care practitioner or a person who operates a group practice of health care practitioners.

Based on a review of the information, I find that Brian Dressler Medicine Professional Corporation, which owns and operates the Clinic, is a health information custodian, as it is a person who operates a group practice, comprised of two physicians who provide specialized health care and treatment to patients, namely, the provision of a comprehensive, supervised methadone program. For the purposes of this Order, I will refer to Brian Dressler Medicine Professional Corporation as the Custodian. The Custodian does not dispute this finding and agrees that it is a health information custodian pursuant to section 3 of the *Act*.

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

Section 12(1)

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.

The Custodian submits that, in these circumstances, it took reasonable steps to ensure that its clients' personal health information was protected against theft, loss and unauthorized use or disclosure. The Custodian states:

> . . . [T]he Clinic took the prudent step of specifically retaining a security firm to establish an appropriate system. The Clinic sought advice from the local police force with respect to the firm and was advised that [the security firm] was a reputable and experienced third-party security firm. The Clinic relied upon the expertise of [the security firm] to recommend and install a secure monitoring system.
>
> The system recommended by [the security firm] was a wireless system. The cameras transmitted the images on one specific band-width within the 2.4Ghz frequency. [The security firm] advises that only a receiver set to that specific frequency, and band-width, could receive and display the image. It is important to note that the system was not connected in any way to a computer or computer network – this is not a case of images being transmitted over the internet.
>
> According to the statement from [the security firm], it is only in recent months that other retail products have been introduced that also use the same frequency range and bandwidth. It was not reasonably foreseeable to the Clinic that with the introduction of rear park assist cameras and monitors into motor vehicles that these images could be received by third parties. We are advised that the security firm was not itself aware of any incident of this nature having ever occurred before. In the absence of any prior notice of such problems and in the absence of prior incidents or any communiqué from the regulator of the Methadone Program (the CPSO), it is unwarranted to suggest that the Clinic breached its obligation set out in s. 12. Obviously, taking a retrospective approach it is apparent that the system was not foolproof, but that is not the applicable test. The threshold of reasonableness does not involve an outcome-based analysis, but rather a prospective analysis based on the information that was available at the time.

Having wrestled with this question, I am sympathetic to the position of the Custodian. While it may be argued that the Custodian did not take reasonable steps to ensure that its clients'

personal health information was protected against theft, loss, unauthorized use and disclosure, I am not prepared to make such a finding at this time.

I believe that the Custodian took the steps it considered to be necessary to comply with section 12(1). For example, it is commendable that the Custodian took steps towards protecting client privacy by not making a permanent record of the video images, and by placing the monitor in the nurses' room, which is a relatively restricted area. I find that these steps were reasonable at the time the surveillance system was installed.

The Custodian states that it had asked the police to recommend a reputable and experienced security firm. However, it appears that the Custodian sought the advice of the police for the purpose of installing a burglar alarm system, *not a video surveillance system*. In the Custodian's submissions, it included a statement from the security firm. The final paragraph of that statement reads,

> [There] is no written work order or contract for the installation of the wireless cameras. When [we] were on site installing the [Custodian's] burglar alarm system[,] we were asked about installing the cameras. The quotations and approval of the camera system [were] done verbally.

I accept that the Custodian most likely asked the security firm to install a "secure" system, but the meaning of "secure" was never spelled out or specifically addressed. Further, for many years, I have made the case that *security* and *privacy* are not one and the same. There is a qualitative difference between seeking advice for a burglar alarm system and seeking advice for a video surveillance system designed to capture sensitive personal information. In future, the Custodian should seek specific expert advice pertaining to the use of a video surveillance system.

Wireless Communication Systems

The particular technology in question is a wireless video surveillance system. Typically, these systems transmit radio signals to receivers attached to television monitors. Wireless transmissions occur in publicly used frequency bands, of which there are a limited number. As a result, the chances of unauthorized reception are relatively high. Therefore, special precautions must be taken to secure these systems, such as encrypting the signal, or, preferably, using a wired system.

I am not suggesting that custodians should become experts in either security or the technology of surveillance. I am, however, suggesting that custodians should be capable of expressing their requirements for any technology dealing with personal health information, and should understand the necessity to inquire as to whether the system being recommended meets those requirements.

It may be argued that this sets too high a bar for custodians, especially in the case of smaller organizations. I do not accept this argument, since I am not expecting custodians to become technical experts. I am expecting custodians to be held to a higher standard than ordinary individuals with respect to the need to protect personal health information, in light of their statutory responsibilities under the *Act*. I may also have higher expectations for larger custodians,

who most likely have access to a broader internal technical skill set. Nonetheless, there is a fundamental base of expectations that I will hold all custodians to.

The Custodian states that only a specifically tuned receiver could receive and display the image, and that the security firm advised that it was not aware of any incident of this nature having ever occurred before. The fact remains that *any* specifically tuned receiver within range of the broadcast could receive and display the image. In my view, the fact that the broadcast and reception equipment was available to be purchased by the Custodian means that any member of the public also could have purchased a compatible receiver at that time. This created a reasonably foreseeable and unacceptable risk of unauthorized viewing of the images, despite the security firm not having specific knowledge of such an instance.

The Custodian states that the system was not connected in any way to a computer or computer network, and that the images were not transmitted over the Internet. In my view, publicly broadcast (unencrypted) wireless transmissions are a functional equivalent of transmission over the Internet (albeit, with a more limited range). The relevant question here is whether appropriate security measures were applied to those transmissions.

With the increasing availability of wireless, mobile back up cameras, the pre-existing risk of unauthorized viewing is increasing, as demonstrated by the events that lead to this order.

With the continuous and rapid evolution of information technology, it is incumbent upon custodians to regularly review and evaluate their systems, from a privacy and security perspective. I do not expect custodians to be experts in the various areas of technology in current usage. However, I do expect custodians to acknowledge their lack of expertise and regularly confer with the appropriate experts to ensure that the systems they use continue to be privacy protective. Had the Custodian implemented such a review, in this case, it is likely that it would have become aware of the increased risks posed by emerging wireless technologies, and taken steps to modify its monitoring system.

Such a privacy and security review need not be an elaborate process. Depending on the circumstances, it may be as simple as a brief meeting with the custodian's service provider, on an annual basis. In my view, a custodian that fails to conduct such regular reviews is likely to fall short of the reasonableness standard in section 12(1) of the *Act*.

I considered ordering the Custodian to conduct a security review of the new, wired, system to determine whether the system is now secure. However, the Custodian has provided me with proof that a security review was already conducted since its installation of the new system. I congratulate the Custodian for proactively undertaking this initiative. Given the rate at which threats to electronic systems increase, such a review should become a regular element of system maintenance. I will address this in the order provision.

Section 12(2)

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.

Based on the above, I find that personal health information was accessed by unauthorized persons, namely the reporter and the private investigator. In addition, it is reasonable to conclude that video images of other clients may have been accessed by unauthorized persons between the time the wireless system was installed in 2004 and its replacement installed in May of 2007.

As noted above, the Custodian posted a notice in its waiting room notifying current patients of the incident, identifying the steps taken by the Custodian to contain the damage and to prevent this type of incident from occurring again; they also provided the contact information of my office. In addition, I note that this incident has received fairly broad coverage in the media. While I recognize that former clients may not become aware of the waiting room notice, on balance I am satisfied that it is likely these individuals would have become aware of the incident by way of the media.

In the circumstances, I find that the Custodian has already fulfilled its obligations to notify affected individuals under section 12(2) of the *Act*.

SUMMARY OF FINDINGS

I have made the following findings in this review:

1. The Custodian created a record of "personal health information" when its surveillance system captured the image of the woman using the washroom, and this information is in "recorded form," under sections 2 and 4 of the *Act*;

2. The Custodian's written records indicating that certain individuals are patients at the Clinic and provided urine samples on particular dates, fall within the definition of "personal health information" that is in recorded form under sections 2 and 4 of the *Act*;

3. The Brian Dressler Medicine Professional Corporation is a "health information custodian" as defined in section 3(1) of the *Act*.

4. The Custodian complied with section 12(1) of the *Act* in that it took 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 use or disclosure.

5. The Custodian has fulfilled its obligations to notify affected individuals pursuant to section 12(2) of the *Act*.

ORDER

The Custodian has already taken remedial action in taking the following steps:

- Immediately containing the privacy breach by turning off the wireless system and replacing it with a more secure wired system;

- Conducting a security review of the new wired system;

- Working with the IPC to draft a notice and posting the notice in its waiting room to advise patients of the privacy breach; and

- Notifying the CPSO of the incident and urging the CPSO to alert other methadone prescribers that wireless camera systems are not secure.

There is only one additional action that remains. Under section 61(1)(g), I order the Custodian to conduct an annual security and privacy review of its personal health information handling systems and procedures to ensure continued compliance with the *Act*. The first review should be completed by June 1, 2008.

COMMISSIONER'S MESSAGE

There are an increasing number of commercially available wireless communication technologies. These include various forms of voice, data and video transmission, as well as reception systems. In a growing number of cases, custodians may collect, use and/or disclose personal health information using such wireless technology for a variety of purposes, including video surveillance. How can a health information custodian take advantage of these new technologies, while still protecting patient privacy?

In this case, a video surveillance camera was installed in a washroom located in a clinic that operates a methadone maintenance treatment program for opiate-dependent patients. According to the CPSO Guidelines, "…urine samples should be obtained…under direct observation." The purpose of direct observation is to ensure that the urine samples provided by patients are not tampered with. This Custodian chose to directly observe patients through the use of live feed video cameras, rather than in person. The patients were aware of the presence of cameras in the washroom and had provided their written consent to being supervised while providing urine samples.

Custodians using wireless communication technologies may learn from this unfortunate yet predictable incident since the use of wireless technology poses a clear risk to privacy. Because wireless communication technology transmits information across many frequency bands, it is susceptible to interference and interception. It operates on the same principles as a commercial radio station. Just as one may accidentally or inadvertently tune in to a distant radio station, personal health information, wirelessly transmitted, without security and privacy precautions, may be "tuned in to" or received by unauthorized individuals. Since there are a limited number of frequency bands legally available for transmission, the risk of inadvertent interception is relatively high, and poses a significant threat to privacy.

Custodians are required under the *Act* to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure. Accordingly, it is my view that if operators of methadone clinics or any other custodians intend to use wireless communications technology in their respective settings, they should only do so if strong, privacy protective precautions have been taken.

Strong security and privacy precautions should involve the use of staff or third parties with appropriate expertise. In my view, one of the first steps a custodian must take is to inform service providers (including external ones such as vendors or internal ones such as IT departments) of its responsibility to protect personal health information under the *Act*. Custodians must understand that while they can outsource services, they cannot outsource accountability. Under the *Act*, one's statutory accountability requires, at a minimum, that the custodian, their agents, and other service providers involved take the following steps (or their equivalent):

- the custodian informs the service provider of the custodian's responsibility to protect personal health information under the *Act*;

- in light of this responsibility, the service provider makes recommendations, providing necessary explanations; in a larger institution, this might involve conducting a Threat Risk Assessment (TRA) and/or a Privacy Impact Assessment (PIA);

- in consultation with the service provider, the custodian makes a decision as to the appropriate system to be installed;

- the service provider installs the system, and the custodian implements supporting policies and procedures; and

- the custodian establishes a schedule for security and/or privacy reviews appropriate for the system involved.

For a large organization, the above steps could involve engaging a third party audit process, while a small practice could easily handle the same objectives less formally.

In light of this incident, custodians should assess the use of all wireless communication technologies for the collection, use and/or disclosure of personal health information and take reasonable steps to minimize the privacy risks inherent in its use.

With respect to video surveillance, while it is possible to secure wireless CCTV systems, it is a far from routine practice and one that places greater technical demands on custodians' staff, since strong encryption or equivalent measures will need to be applied. Directly connected (wired) video systems are generally more secure and easier to maintain.

Therefore, custodians who use video surveillance should either use a wired surveillance system, which inherently prevents interception, or a wireless one with appropriate measures, such as strong encryption, to preclude unauthorized access. Nothing short of this will be acceptable.

Lastly, I strongly urge all custodians to regularly and proactively review their privacy and security policies and procedures relating to the use of wireless communication technologies to ensure that whatever technology they use is effective in minimizing the significant risk to privacy posed by its use.

June 7, 2007

Ann Cavoukian, Ph.D.
Commissioner

Date