



Privacy and Security Challenges in an EHR World – *What are We Waiting For?*

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario**

**Shared Risks, Shared Standards
Sunnybrook Health Sciences Centre**

October 23, 2007



Presentation Outline

- 1. EHRs in Ontario*
- 2. The Promise and the Peril*
- 3. Attitudes Toward EHRs*
- 4. Technology-Related Health Orders*
- 5. Conclusions*



The Development of an EHR in Ontario

Where are We?



Where Ontario Ranks in the Development of EHR

Province/Territory	Anticipated Progress to March 31, 2008
PEI	Completion
Alberta	Completion
Northwest Territories	Adoption
British Columbia	Implementation
Saskatchewan	Implementation
Newfoundland	Implementation
Quebec	Implementation
Nova Scotia	Implementation
New Brunswick	Implementation
Manitoba	Planning
Ontario	Planning
Yukon	Planning
Nunavat	Planning



Alternatives to Provincial EHR

I am exploring two alternatives:

1. HealthVault – Internet-based product that allows patients to develop and control access to their own EHRs; working with Microsoft to obtain an account here in Canada; UHN has agreed to help populate my account, as well as Sunnybrook;
2. EHR based on the Shared Information Management Services (SIMS) network – working with UHN and Sunnybrook to pilot test my own EHR.



The Promise and the Peril

- More efficient and effective delivery of health care service; can save lives; enhance the quality of life;
- Prevent, detect and investigate privacy breaches (e.g., anonymization, user authentication, access controls, and audit logs);
- But not properly implemented, new technologies can have an adverse impact on privacy;
- Many high profile privacy and security breaches have been directly related to the improper implementation of the technologies in play.



Canadians' Attitudes Towards EHRs

- Office of Health and the Information Highway, Health Canada reviewed public opinion polls on the use of information and communications technology in the health sector (2002);
- Review suggests Canadians would welcome expanded role for information technologies in the health sector, provided that privacy and autonomy are protected;
- 9 in 10 Canadians from all regions of the country support the development of information systems that would make it easier to access and share information;
- Canadians have serious fears, however, about the erosion of their privacy and doubts about the security of the Internet.



Public Opinions

- **80%** of Canadians rate EHRs as a strong improvement over paper records in terms of the effectiveness for all those involved in the health care system and for the system overall;
- The most frequent reasons for supporting the EHR:
 - increased access to and availability of health records;
 - a faster, more efficient health system;
 - cost-effectiveness;
- **84%** agree that timely and easy access to personal health information is integral to the provision of quality health care.

— EKOS Survey, 2003/2004



Most Recent Poll

- In 2007, Canada Health Infoway, the federal Privacy Commissioner and Health Canada joined together to updated previous surveys;
- Public support for and comfort with the EHR increased to **90%** — an all time high;
- **30%** indicated that they had some interaction with the EHR – this group was even more supportive than others;
- A number of measures, including sanctions for inappropriate use, would increase the public's confidence and comfort with the EHR.



Technology-Related Orders Under *PHIPA*

- Health Order No. 2 (HO-02)
 - Unauthorized Access
- Health Order No. 4 (HO-04)
 - Mobile Devices
- Health Order No. 5 (HO-05)
 - Wireless Technology



Health Order No. 2:

Unauthorized Access Results in Order

- **Health Order No. 2** (HO-02) showed that the hospital's policies and procedures failed to prevent ongoing privacy breaches by an employee, even after the hospital became aware that such breaches had occurred repeatedly;
- Even when the patient alerted the hospital to her concerns upon admission, the staff did not recognize the obvious threat to privacy posed by the estranged husband and his girlfriend- both employees of the hospital;
- Staff only recognized the threat to the physical security of the patient, not the threat to her privacy;
- After learning about the breach, the hospital was more concerned about the employee's right to due process (Human Resources Policy) than the patient's right to privacy;
- Hospitals can have both – but HR cannot trump privacy.



You are attempting to access what is considered to be a VIP patient or patient whose information has been deemed highly sensitive by the TOH Chief Privacy Officer.

Any attempt to view VIP or highly sensitive patients is closely monitored for potential violations of patient privacy.

The monitor will only be triggered if you proceed beyond this point.
Do you wish to continue?



Commissioner's Findings

- After receiving the privacy complaint, the hospital put a privacy/VIP flag on the patient's electronic medical record – but the nurse continued to access the patient's record;
- Found that the hospital had not taken steps that were reasonable in the circumstances to ensure that the personal health information was protected against theft, loss and unauthorized use or disclosure;
- Hospital was ordered to review its practices and procedures to ensure that human resource issues did not trump privacy;
- Hospital was ordered to implement a protocol that would require immediate steps to be taken upon being notified of an actual or potential privacy breach.



Health Order No. 4


Stolen Laptop Results in Order

- **Health Order No. 4** (HO-04) resulted from a hospital not having adequate policies and procedures to permit compliance with *PHIPA*;
- In spite of the known high risk of loss or theft, extremely sensitive personal health information was transported on a portable device (laptop) without adequate safeguards;
- This is clearly unacceptable, more than two years after *PHIPA* came into force.



Encrypting Personal Health Information on Mobile Devices

- Why are login passwords not enough?
- What is encryption?
- What are the options?
 - Whole disk (drive) encryption
 - Virtual disk encryption
 - Folder or Directory encryption
 - Device encryption
 - Enterprise encryption



Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 12
May 2007

Encrypting Personal Health Information on Mobile Devices

Section 12 (1) of the *Personal Health Information Protection Act, 2004 (PHIPA)* sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) 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 Office of the Information and Privacy Commissioner/Ontario recognizes that the delivery of health care may require the use of PHI outside of the workplace, and that such PHI may most effectively be transported and used in electronic form. Notwithstanding the ease of use and portability of electronic documents, it is still important that only the minimum necessary data be transported in this manner.

Because of the high incidence of loss or theft of mobile devices such as laptop computers, personal digital assistants (PDAs), or flash drives, custodians need to ensure that personal health information that is stored on mobile devices is encrypted. When encryption is implemented properly, it renders PHI safe from disclosure. The availability of encryption means that it is easier to safeguard electronic records of PHI than it is to safeguard paper-based records when being transported.

This fact sheet is intended for health information custodians who store PHI on mobile devices. However, it is also relevant to anyone who stores personal information on a mobile device. If you are unsure of the meaning of these guidelines, please consult a computer systems security expert to determine how to apply this fact sheet to the information in your care. In many cases, encryption can be as easy as installing a simple program and implementing proper key management for the system.

Why are login passwords not enough?

It is not acceptable to rely solely on login passwords to protect PHI on devices that are easily stolen or lost. "Strong" login passwords will prevent casual access to data on a device, but may not prevent access by knowledgeable thieves. Strong login passwords are usually characterized by:

- No dictionary words;
- A combination of letters, numbers and symbols;
- Eight or more characters, with 14 or more being ideal.

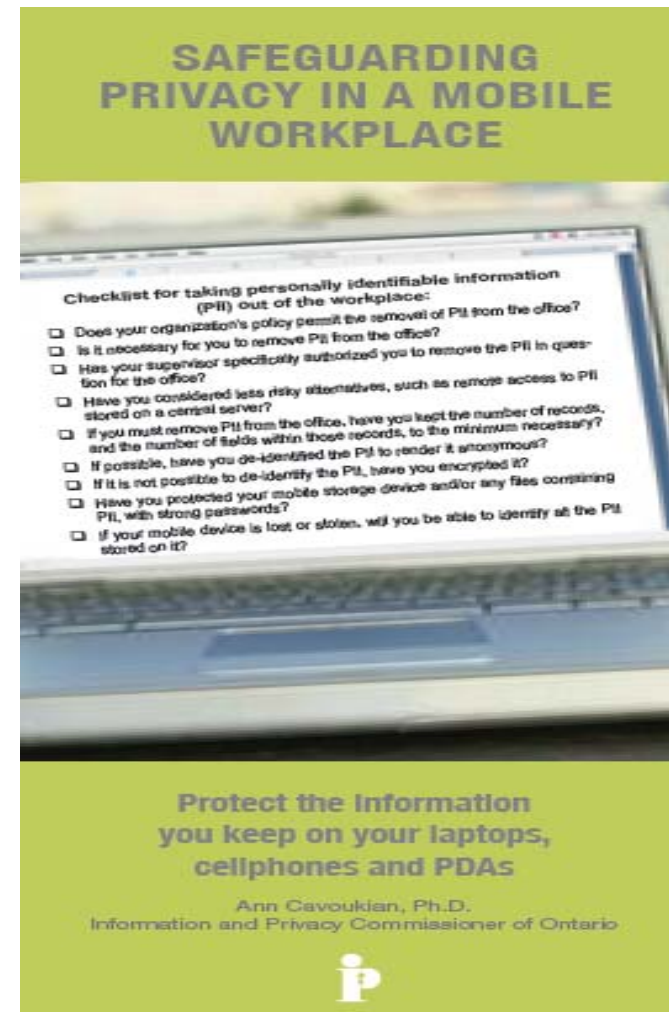
For example, "LetMeIn" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25"



Brochure on Mobile Devices

Safeguarding Privacy In A Mobile Workplace

- Does your organization's policy permit the removal of PII from the office?
- Is it necessary for you to remove PII from the office?
- Has your supervisor specifically authorized you to remove the PII in question for the office?
- Have you considered less risky alternatives, such as remote access to PII stored on a central server?
- If possible, have you de-identified the PII to render it anonymous?
- If it is not possible to de-identify the PII, have you encrypted it?
- If your mobile device is lost or stolen, will you be able to identify the PII stored on it?





Commissioner's Findings

- The laptop contained highly sensitive health information including HIV status;
- The researcher admitted that he did not need identifiable health information for the purposes of the research – it should not have been on the laptop in the first place;
- Although the hospital's research protocol required researchers to only use coded information, the hospital did not take steps to ensure that researchers actually followed this protocol;
- The Hospital was ordered to either de-identify or encrypt all personal health information before allowing it to be removed from the workplace;
- Where personal health information is stored on a mobile, portable device, it must be encrypted.



Health Order No. 5

Wireless Technology Results in Order

- **Health Order No. 5** (HO-05) resulted from a methadone clinic that installed a wireless video surveillance system in its washroom to monitor patients providing urine samples;
- Video images were intercepted by a wireless rear view backup camera in a car outside of the clinic;
- Clinic immediately agreed to shut down the cameras and replaced the wireless surveillance system with a more secure wired system.



Commissioner's Message

- Although the clinic did not video tape the images captured by the surveillance system, since the system created digital data that were transmitted via air waves, the IPC determined that these digital images were, in fact, records of personal health information subject to *PHIPA*;
- Custodians should either use a wired system which inherently prevents unauthorized interception, or a wireless one with strong security measures such as encryption, to preclude unauthorized access;
- In response to this incidence, all health information custodians should assess the use of their wireless communication technology for the collection, use and/or disclosure of personal health information;
- In light of the evolving technological landscape, health information custodians should regularly and proactively review their privacy and security policies and procedures, and technologies employed;
- IPC has issued a new Fact Sheet: *Wireless Communications Technologies: Video Surveillance Systems*. A second Fact Sheet on Wireless Technology will follow.



Fact Sheet

Wireless Communication Technologies: Video Surveillance Systems

- Special precautions must be taken to protect the privacy of video images;
- No covert surveillance should be conducted;
- Clearly visible signs should be posted indicating the presence of cameras and the location of their use;
- Recording devices should not be used;
- Only minimum number of staff should have access to the video equipment;
- Staff should receive technical training on the privacy and security issues;
- Regular security and privacy audits should be conducted, on an annual basis.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 13
June 2007

**Wireless Communication Technologies:
Video Surveillance Systems**

Section 12(1) of the *Personal Health Information Protection Act (PHIPA)* sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) 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.

In a widely publicized incident, for which an Order was issued – HO-005 – images of a patient giving a urine sample in a washroom were being accessed by a wireless mobile rear-assist parking device (“back up camera”), in a car parked near a clinic. The patient was attending a methadone clinic in which patients were required to give urine samples under direct observation. The clinic was unaware that such an interception was even possible.

Closed Circuit Television (CCTV) or video surveillance cameras are being used in the Ontario health sector for a range of purposes ranging from building security to observational research. Typically, these uses increase efficiency or help prevent negative patient outcomes. The unintended consequence of video surveillance, however, regardless of its primary function, is often an invasion of personal privacy. This risk is increased if wireless communication technology is used without adequate protection.

This fact sheet is intended to address privacy issues that arise from the use of wireless communication technologies. The standard established in Order HO-005 is that health information custodians in Ontario should not use wireless video surveillance cameras without strong security and privacy precautions. Any organization that chooses to use wireless communication technology to transmit personally identifiable information needs to take appropriate proactive measures to protect the privacy of individuals.

What is wireless video surveillance technology?

Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to television monitors, not computer screens. The most common commercial use of this equipment is for building security. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but will allow unauthorized access unless special precautions are taken. Health information custodians must ensure that no one other than specifically authorized staff have the capability of viewing patient images.



Fact Sheet

Wireless Communication Technologies: Safeguarding Privacy & Security

- A good starting point for understanding the impact of technological change is to regularly re-examine past assumptions and decisions;
- Any time wireless technology is used to transmit personal information, that information must be strongly protected to guard against unauthorized access to the contents of the signal.



Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 14
August 2007

Wireless Communication Technologies: Safeguarding Privacy & Security

Taking Care

We are fast approaching the point where it is reasonable to assume that any device that creates or stores data either has, or is connected to, some form of embedded wireless capability. Cellphones and personal digital assistants (PDAs) are increasingly sophisticated, often combining multiple wireless technologies in a single device.

Wireless technologies can reduce costs, increase efficiencies, and make important information more readily and widely available. In the health care sector, for example, wireless data communications now make it possible for paramedics to send cardiac images and data directly to cardiologists, significantly reducing wait time to treatment.

Clearly, the benefits of wireless communications are many. But, there are also risks. Without appropriate safeguards, transmitting data wirelessly can be like using an open filing cabinet in a waiting room. In fact, this Office just recently issued an Order about a case where unauthorized viewers had inadvertently intercepted wireless video images of patients in a washroom providing urine samples.

This Fact Sheet addresses privacy issues arising from the use of wireless technologies, expanding on Fact Sheet #13, *Wireless Communication Technologies: Video Surveillance Systems*.

The *Personal Health Information Protection Act* (PHIPA), the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) set out requirements for the protection of personal information, including information in electronic form.

In general, compliance with these Acts requires that those responsible take reasonable measures to protect personal information, which may include physical safeguards, using role-based access to personal information, or technological measures such as encryption.

The transmission of personal information in electronic form, particularly through the use of wireless technologies, means adding "data-in-motion" to "data-at-rest" as a category of data to protect, and adds another layer of complexity to compliance with these Acts.

A good starting point for understanding the impact of technological change or new developments is to regularly re-examine past assumptions and decisions. A reasonable precaution is one that any prudent and privacy conscious individual or institution would take. For example, there was a time when it was reasonable to browse the web and download files without



Conclusions

- EHRs have serious advantages, as well as challenges;
- The public generally supports EHRs, but wants to ensure that their privacy is well protected;
- Privacy protective features of systems that are currently in general use must be enhanced;
- I look forward to working with the government to expedite the development and implementation of EHRs in Ontario.



How to Contact Us

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca