Health Information Technology:

A Canadian Approach to Privacy and Security

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Workgroup for Electronic Data Interchange

September 18, 2008

Presentation Outline

1. *Who Are We?*
2. *Personal Health Information*
3. *Differing Approaches to Privacy*
4. *Electronic Health Records (EHR)*
5. *Personal Health Records (PHR)*
6. *Markle Foundation Framework*
7. *Technology-Related Orders Under PHIPA*
8. *Positive-Sum NOT Zero-Sum*
9. *Transformative Technologies*
10. *Conclusions*

Who Are We?

Three Statutes in Ontario

The role of the Information and Privacy Commissioner of Ontario (IPC) is set out in three statutes:

- *Freedom of Information and Protection of Privacy Act* (FIPPA);
- *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA);
- *Personal Health Information Protection Act* (PHIPA).

Responsibilities

Under its statutory mandate, the Commissioner is responsible for:

- investigating privacy complaints;
- resolving appeals from refusals to provide access to information;
- ensuring that organizations comply with the access and privacy provisions of the *Acts*;
- educating the public about Ontario's access and privacy laws; and
- conducting research on access and privacy issues, and providing advice and comment on proposed government legislation and programs.

The Commissioner has strong order-making power, under all three statutes.

Personal Health Information

Unique Characteristics of Personal Health Information

- Highly sensitive and personal in nature;
- Must be shared immediately and accurately among a range of health care providers for the benefit of the individual;
- Widely used and disclosed for secondary purposes that are seen to be in the public interest (e.g., research, planning, fraud investigation, quality assurance);
- Dual nature of personal health information is reflected in *PHIPA*, and all other health privacy legislation.

Privacy Risks: Unauthorized Disclosures

3rd Party disclosures, not authorized by the patient, may threaten the integrity of the system:

- Fear of stigmatization, discrimination, loss of employment opportunities, denial of insurance, denial of housing;

A 2007 EKOS Canada Survey:

- Estimated that 1.2 million Canadians have withheld personal information from a health care provider because of concerns over who the information would be shared with, or how it might be used;

California HealthCare Foundation survey:

- One in six people (50 million) engage in privacy-protective behavior to shield themselves from misuse of their information.

Privacy-Protective Behaviors

- Multiple doctoring;
- Out of pocket payment;
- Avoiding testing;
- Avoiding treatment;
- Lying or withholding information from providers;
- Asking providers to misrepresent diagnosis in records;
- Inaccurate and incomplete information far less helpful for primary purposes, such as treatment, and secondary purposes such as research.

Differing Approaches to Privacy

Privacy Laws
Canada, United States and Europe

Canada

- Public sector privacy laws: federal, provincial and municipal;
- Private sector privacy laws: (Federal) *Personal Information Protection and Electronic Documents Act (PIPEDA)*; (Provincial) Quebec, British Columbia, Alberta;
- Health sector privacy laws: (Provincial) Ontario, Manitoba, Saskatchewan, Alberta.

United States

- Public sector privacy law: (Federal) *Privacy Act;*
- Sectoral privacy laws;
- Safe Harbor Agreement;
- Health sector privacy law: (Federal) *Health Insurance Portability and Accountability Act (HIPAA).*

United States: Safe Harbor Privacy Principles

1. Notice
2. Choice
3. Onward Transfer
4. Security
5. Data Integrity
6. Access
7. Enforcement

Canada's Fair Information Practices

1. **Accountability**
2. **Identifying Purposes**
3. **Consent**
4. **Limiting Collection**
5. **Limiting Use, Disclosure, Retention**
6. **Accuracy**
7. **Safeguards**
8. **Openness**
9. **Individual Access**
10. **Challenging Compliance**

Personal Information Protection and Electronic Documents Act,
www.privcom.gc.ca/legislation/02_06_01_01_e.asp

HIPAA Privacy Rule

- Requires Covered Entities to provide notice to consumers of their rights and protections;
- Requires Covered Entities to provide consumers with copies of or access to their information if requested;
- Permits health care providers to use and disclose patient data, without consent, for treatment, payment and health care operations;
- Puts limits on other uses and disclosures of patient information;
- Requires providers and other Covered Entities to obtain patient authorization for disclosures not expressly permitted by the Privacy Rule;
- Sets out rules for disclosures to researchers, law enforcement, and public health officials without consent or authorization;
- Provides oversight and enforcement mechanisms.

HIPAA Challenges

- US Department of Health and Human Services Office for Civil Rights reports that since the Privacy Rule went into effect in 2003, an estimated 32,595 to 42,000 voluntary complaints have been received;
- As of July 2007, corrective action has been taken in fewer than 5,000 cases;
- To date, there has been only one “resolution agreement” between HHS and Providence Health and Services;
- To date, no civil penalties and only a handful of criminal prosecutions have resulted from the Privacy Rule;
- Many Covered Entities remain confused about what the Privacy Rule does and does not allow (see *Policy Overview*, *Common Framework for Networked Personal Health Information*, *Markle Foundation*).

www.connectingforhealth.org

Ontario's Personal Health Information Protection Act (PHIPA)

- Applies to organizations and individuals involved in the delivery of health care services (both public and private sector);
- The only health sector privacy legislation in Canada based on consent: implied consent within healthcare providers "circle of care," otherwise, express consent is required;
- The only health sector privacy legislation that was declared to be substantially similar to Canada's federal private sector law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA);
- *PHIPA* is undergoing its mandatory three year review and the consensus among stakeholders is that *PHIPA* is operating very well;
- Challenge with *PHIPA* is how it is being interpreted and applied by health information custodians.

Requirements of *PHIPA*

- Requires consent for the collection, use and disclosure of PHI, with necessary but limited exceptions;
- Requires that PHI be kept confidential and secure;
- Requires a statement of information practices be made available to the public;
- Requires notification of patients when there is a privacy breach;
- Codifies individuals' right to access and request correction of their own PHI;
- Gives patients the right to instruct health information custodians not to share any part of their PHI with other health care providers;
- Establishes clear rules for the use and disclosure of PHI for secondary purposes including fundraising, marketing and research;
- Ensures accountability by granting an individual the right to complain to the IPC about the practices of a health information custodian; and
- Establishes remedies for breaches of the legislation.

Electronic Health Records (EHR)

The Development of an EHR in Ontario

Where are we?

… not very far

Where Ontario Stands in the Development of EHR

- Given the time and resources that have been devoted to e-health initiatives, Ontario is not as far along in the development and implementation of EHR as it should be;
- Ontario continues to lag behind most of the other provinces and communication among health care providers is still very limited;
- Several initiatives are complete or under development but we are still a long way from an integrated EHR system.

Personal Health Records (PHR)

PHRs – Alternative to an EHR?

- New PHR services are being developed and implemented to allow patients to integrate their own personal health information into one location;
- PHRs are offered by private sector organizations such as Microsoft and Google;
- PHRs can be networked with other health information systems (e.g. laboratory information systems, pharmaceuticals, x-rays, etc.);
- To the extent that PHRs allow patients to integrate relevant information and share this information to their health care providers, they are being characterized as an alternative to an interoperable EHR which all provincial governments are spending millions of dollars developing;
- The development of PHRs has the potential to transform the delivery of health care and may overtake and replace the development of EHRs.

Three Examples of PHRs

I am exploring three alternatives:

1. **MyChart –** A patient portal that allows the patient to view their personal health information (PHI) stored in Sunnybrook Hospital's electronic medical records;

2. **HealthVault –** Internet-based product that allows patients to develop and control access to their own PHI. I have populated an account with my medical records;

3. **Google Health –** Internet-based product that allows patients to enter their PHI or have their health care providers upload their PHI from compatible systems. Patient can also control who has access to their PHI.

Markle Foundation Framework

Markle Foundation Framework

- **Connecting for Health** Work Group on Consumer Access Policies for Networked Personal Health Information is a public-private collaboration engaging over 100 organizations that represent all the major components of the health sector, operated and financed by the Markle Foundation;
- Developed a framework that proposes a set of practices that encourage appropriate handling of personal health information as it flows to and from PHRs and similar applications or supporting services;
- In the US, providers of PHRs generally are not covered by health privacy legislation and once the consumer consents to the disclosure of their personal health information from a covered entity, that information is no longer subject to legislative protections;
- The lack of consistent rules and complex consumer notices are confusing for consumers;
- The Markle Foundation Framework was intended to fill this privacy policy void by encouraging a set of common practices that manage risk acceptably for consumers, health data sources, and consumer access services.

Connecting for Health Core Principles

1. Openness and transparency (Openness)
2. Purpose specification (Identifying Purposes)
3. Collection limitation and data minimization (Limiting Collection)
4. Use limitation (Limiting Use, Disclosure and Retention)
5. Individual participation and control (Consent)
6. Data quality and integrity (Accuracy)
7. Security safeguards and controls (Safeguards)
8. Accountability and oversight (Accountability)
9. Remedies (Challenging Compliance)

Features of Framework

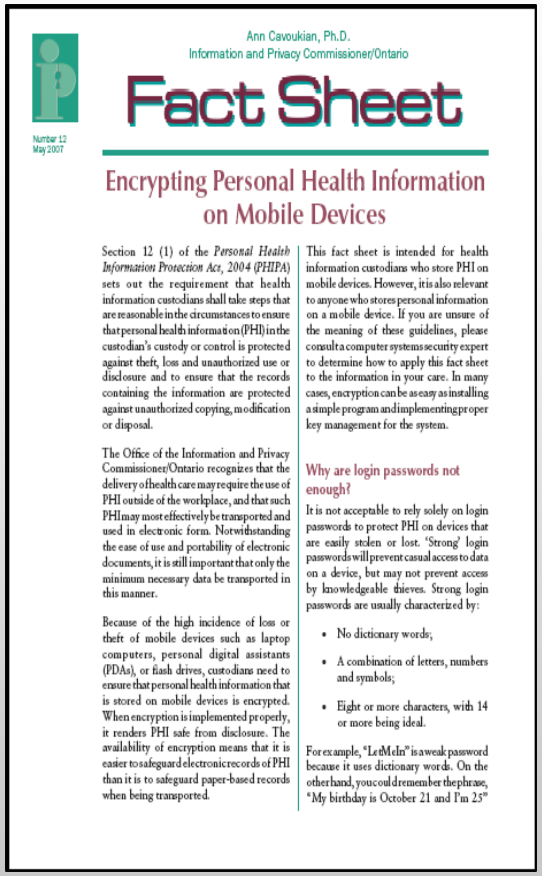
- Very patient/consumer centric approach;
- Recommends strong privacy best practices;
- Envisions PHRs working in conjunction with EHRs;
- Overarching privacy principles are similar to those set out in Canada Health Infoway's (CHI) Privacy and Security Architecture for interoperable EHRs;
- Whereas CHI's framework allows for a range of privacy and security options to be determined by each jurisdiction, the Markle framework is more prescriptive in terms of recommending specific practices that are privacy protective;
- Markle framework also recommends harmonization of privacy best practices across all consumer access services.

Technology-Related Orders Under PHIPA

Guidance for Custodians

- The IPC provides guidance to health information custodians on technology-related privacy issues through issuing orders;
- 3 of the 5 orders issued to date have implications for technology;
- Unauthorized access to a patient's electronic medical record resulted in Order #2;
- A stolen laptop containing unencrypted patient information resulted in Order # 4;
- The transmission of images of a patient providing a urine sample in a methadone clinic, through wireless video surveillance technology resulted in Order #5.

IPC Fact Sheets



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.

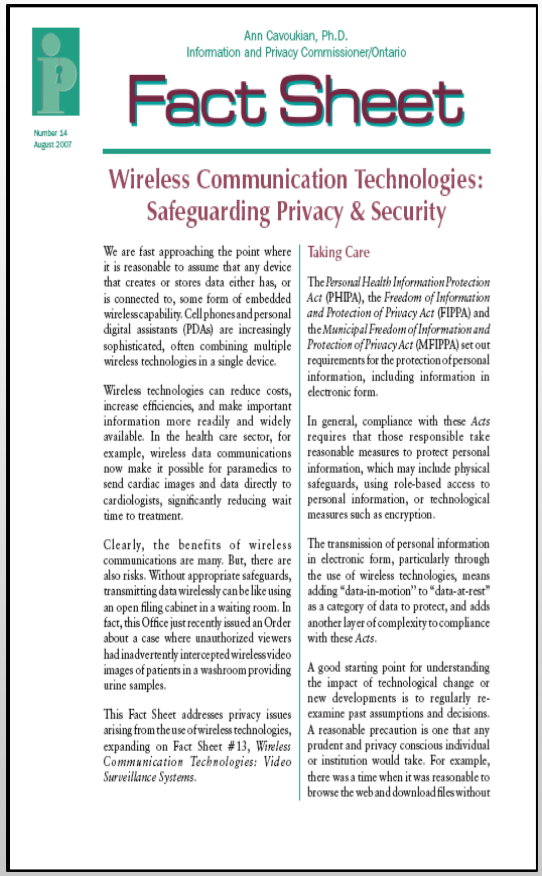
Why are login passwords not enough?

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"

www.ipc.on.ca/images/Resources/up-fact_12e.pdf



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

Fact Sheet

Number 14
August 2007

Wireless Communication Technologies: Safeguarding Privacy & Security

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. Cell phones 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*.

Taking Care

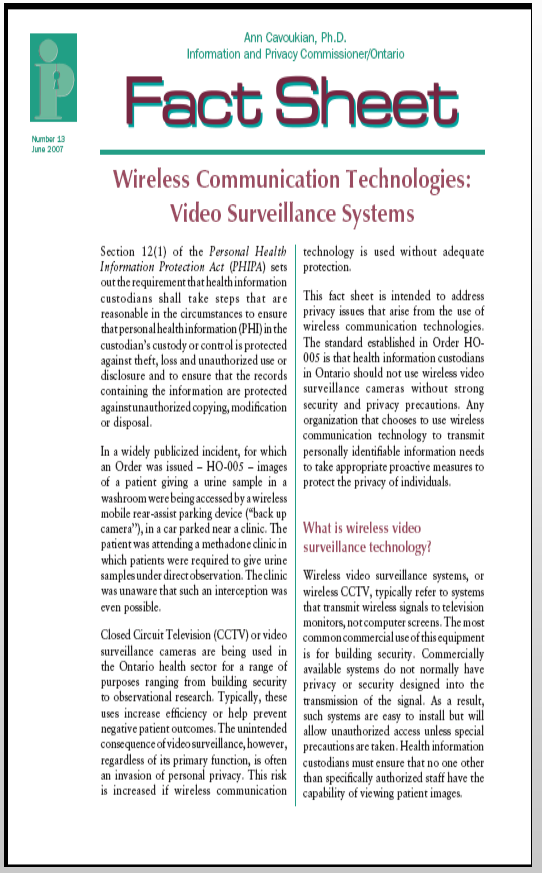
The *Personal Health Information Protection Act* (PHIPA), the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) set out requirements for the protection of personal information, including information in electronic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

www.ipc.on.ca/index.asp?navid=46&fid1=645



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.

www.ipc.on.ca/images/Resources/up-fact_13_e.pdf

Positive-Sum
NOT
Zero-Sum

Positive-Sum Model

Change the paradigm
from a zero-sum to
a positive-sum model:
Create a "win-win" scenario,
not an "either/or"
involving unnecessary
trade-offs

Privacy by Design: "Build It In"

- Build in privacy – up front, into the design specifications; into the architecture; if possible embed privacy right into the technology used – ***bake it in***;
- Assess the risks to privacy: conduct a privacy impact assessment; follow up with annual privacy audits;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- Use privacy-enhancing technologies (PETs) where possible: give people maximum control over their own data.

Transformative Technologies

Transformative Technologies

Surveillance Technology + Positive-Sum Paradigm + Privacy Enhancing Technology =

<u>Transformative Technologies</u>

Common characteristics of Transformative Technologies:

- Minimize the unnecessary collection, disclosure, use and retention of personal data;
- Empower individuals to participate in the management of their own personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in personal data governance structures;
- Promote/facilitate the commercialization and adoption of these technologies.

Conclusions

- Similar privacy principles apply in both Canada and in the US, but with very different approaches to enforcement;
- In Ontario, IPC orders interpret the law and set the standard of practice to ensure compliance with the requirements of *PHIPA*;
- New technologies such as EHRs and PHRs can pose a threat to privacy unless privacy is built into their design and implementation – we call this "privacy by design;"
- Adopting a positive-sum paradigm of privacy AND security or functionality, where privacy is built right into the design, is a far more productive approach, leading to a "win/win" scenario;
- Transformative technologies maintain the functionality of technologies, yet transform them to operate in a privacy-protective manner by embedding privacy into their design.

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