



*Why Your Fiduciary Responsibilities  
as Board Members Extend to  
Protecting Your Clients' Privacy*

**Ann Cavoukian, Ph.D.**

**Information and Privacy Commissioner  
Ontario**

**University Health Network  
Board of Directors**

*July 18, 2007*



# Privacy Defined

## Informational Privacy: Data Protection

- Freedom of choice, personal control, informational self-determination;
- Control over the collection, use and disclosure of recorded information about an identifiable individual;
- An organisation's responsibility for data protection and the safeguarding of personally identifiable information, in its custody or control.



# What Privacy is Not

**Security  $\neq$  Privacy**



# Privacy and Security: *The Difference*

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation



## **Security:**

Organizational control of information through information systems

- Privacy; Data Protection
- Fair Information Practices



# Fair Information Practices: *A Brief History*

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980);
- European Union Directive on Data Protection (1995/1998);
- CSA Model Code for the Protection of Personal Information (1996); Personal Information Protection and Electronic Documents Act (2000);
- United States Safe Harbor Agreement (2000);
- Global Privacy Standard (2006).



# Canada's Fair Information Practices

- **Accountability**
- **Identifying Purposes**
- **Consent**
- **Limiting Collection**
- **Limiting Use,  
Disclosure, Retention**
- **Accuracy**
- **Safeguards**
- **Openness**
- **Individual Access**
- **Challenging  
Compliance**

*CSA Model Code for the Protection of Personal Information*  
(Privacy Code) CAN-CSA Q830 1996

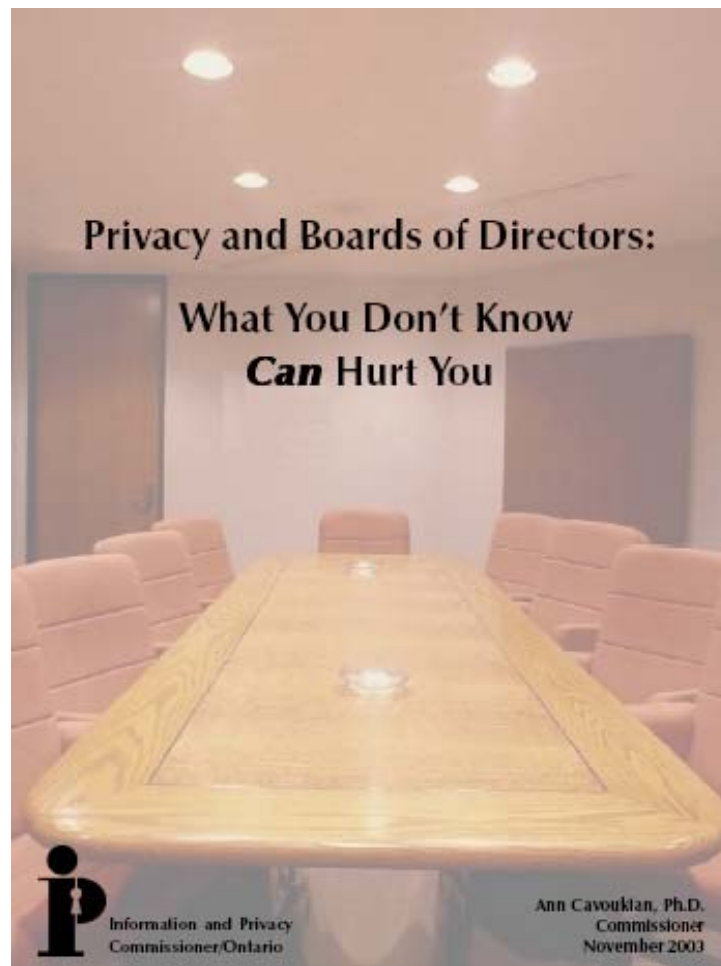
[www.csa.ca/standards/privacy/code/](http://www.csa.ca/standards/privacy/code/)



# Good Governance and Privacy

## IPC Publication:

- Guidance to corporate directors faced with increasing responsibilities and expectation of openness and transparency;
- Privacy among the key issues that Boards of Directors must address;
- Potential risks if Directors ignore privacy;
- Great benefits to be reaped if privacy included in a company's business plan.



[www.ipc.on.ca/docs/director.pdf](http://www.ipc.on.ca/docs/director.pdf)



# Protecting Patient Privacy

- Certain laws and regulations impose a “duty of care” on businesses to collect and manage personal information by providing notice, obtaining consent, and providing access and correction rights:
  - Health Insurance Portability and Accountability Act (U.S.);
  - Sarbanes-Oxley (U.S.);
  - Gramm-Leach-Bliley;
  - *PHIPA* (Ontario).





# *Personal Health Information Protection Act (PHIPA)*

- Applies to organizations and individuals involved in the delivery of health care services in both the public and private sectors;
- The only health sector privacy legislation in Canada based on consent: implied consent within the “circle of care,” otherwise, express consent;
- The only health sector privacy legislation that was declared to be substantially similar to the federal *PIPEDA* legislation, in 2005;
- The only legislation in Canada with a mandatory breach notification requirement.



# Why UHN?

Recognized as a leader in privacy and in the development and implementation of new technology and privacy practices among hospitals in Ontario;

- **CIO – Matt Anderson** – recognized nationally for his significant contributions to e-health (e.g., ambulatory electronic patient record);
- **Former CPO – Miyo Yamishita** – recognized for putting UHN on the map with its innovative privacy program and for her ongoing work in the health care sector;
- **Current CPO – Abigail Carter** – recognized for her ongoing efforts in keeping UHN compliant with *PHIPA* and for meeting privacy challenges associated with the adoption of new technology.



# Consequences of Inadequate Attention to Privacy

- Privacy breaches and violations of *PHIPA*;
- Damage to a hospital's reputation, image, and business relationships (unwanted media, notification of patients);
- Psychological and economic harm to patients (identity theft, loss of insurance, employment, housing, etc.);
- Patients may withhold consent for the collection, use and disclosure of personal health information, making the effective delivery of care more challenging;
- Unhappy patients can create an administrative burden for hospitals (e.g., unnecessary lock box requests, complaints to the IPC, etc);
- Dealing with a privacy breach, after the fact, can be time consuming and expensive (e.g., breach notification).



# 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 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;
- 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 than the patient's right to privacy;
- Hospitals can have both –but HR cannot trump privacy.



# Building A Culture of Privacy

- A culture of privacy enables sustainable action throughout an organization by providing people with a similarity of approach, outlook, and priorities;
- The importance of privacy must be a message that comes from the top;
- One way of getting the message across is by devoting adequate resources to privacy programs;
- Privacy must be woven into the fabric of the day-to-day operations of an organization.



# Weaving Privacy into Day-to-Day Operations

- On-going privacy training and awareness program (new staff training; refresher training for existing staff, identifying new threats to privacy, finding new technology solutions);
- Policies and procedures for maintaining privacy must be clearly articulated, and individuals must know how to apply them in their day-to-day work;
- Privacy must form part of the performance standard for individuals working in the information-intensive health care sector.



# Health Order No. 4


## *Stolen Laptop Results in Order*

- Despite the known high risks of loss or theft, personal health information was transported out of a hospital on a portable device (a laptop) by a physician, without safeguards;
- The Hospital was ordered to either de-identify or encrypt all personal health information before allowing it to be removed from the workplace;
- **Health Order No. 4** (HO-04) created the standard of practice expected regarding the removal of identifiable health information from a healthcare facility – if it's not encrypted, it's not in compliance with *PHIPA*.



# 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"





# 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;
- The Clinic was ordered to strongly encrypt all wireless signals if wireless video technology was to be utilized, and to review encryption practices on an annual basis;
- The standard of practice created by this Order was that if healthcare providers choose to use wireless technology, then they must encrypt – strongly.



# Fact Sheet:

## *Wireless Communication Technologies*

- 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.



# Stressing the 3 C's

## **Consultation**

- Opening the lines of communication with the health care sector and seeking their views;

## **Co-operation**

- Not confrontation in resolving complaints – taking a non-adversarial approach;

## **Collaboration**

- Working together to find joint solutions.



# What Can Boards Do to Help Foster a Culture of Privacy?

- Ensure some privacy expertise on the Board of Directors;
- Designate one person on the Board of Directors who is responsible for privacy;
- Make privacy compliance part of management performance evaluation and compensation package;
- Ask management to undertake privacy self-assessments and privacy audits;
- Ask management to demonstrate compliance with legislation and best practices in order to reap the benefits of good privacy practices and avoid unnecessary breaches.



# Conclusions

- UHN is recognized as a leader, but must remain vigilant about safeguarding privacy;
- Hospitals must have an on-going privacy training and awareness program (new staff training; refresher training for existing staff, identifying new threats to privacy, finding new technology solutions);
- Adequate resources must be devoted to privacy programs;
- Privacy must be woven into the fabric of the day-to-day operations of a hospital;
- *Importance of privacy must come from the top* – set the stage as board members by sending a clear message.



# How to Contact Us

**Ann Cavoukian, Ph.D.**

**Information & Privacy Commissioner of Ontario**

**2 Bloor Street East, Suite 1400**

**Toronto, Ontario, Canada**

**M4W 1A8**

**Phone: (416) 326-3333 / 1-800-387-0073**

**Web: [www.ipc.on.ca](http://www.ipc.on.ca)**

**E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)**