



The Impact of New Technology in Health Care on Privacy

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario**

**Ontario College of Social Workers
and Social Service Workers**

June 18, 2008



Presentation Outline

- 1. Personal Health Information*
- 2. Personal Health Information Protection Act (PHIPA)*
- 3. Technology-Related Orders Under PHIPA*
- 4. Electronic Health Records in Ontario*
- 5. Radio Frequency Identification (RFID)*
- 6. Think “Positive-Sum” not “Zero-Sum”*
- 7. Conclusions*



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 in the Context of Health Care

- Privacy is not a new issue in the health care context
 - all medical staff are well aware of the privacy issues;
- *PHIPA* was drafted in a manner such that privacy would not impede the delivery of health care services;
- Health information custodians may imply consent for the collection, use and disclosure of personal health information for the delivery of health care services;
- Express consent is required when personal health information is disclosed to a person who is not a health information custodian, or for a purpose other than the delivery of health care services.



*Personal Health
Information Protection
Act (PHIPA)*



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;
- 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).



Mandate of the Legislation

- Requires consent for the collection, use and disclosure of PHI, with necessary but limited exceptions;
- Requires that health information custodians treat all PHI as confidential and keep it secure;
- Codifies an individual's right to access and request correction of his/her own PHI;
- Gives a patient the right to instruct health information custodians not to share any part of his/her PHI with other health care providers;
- Establishes clear rules for the use and disclosure of personal health information 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.



Permissible Disclosures:

Safety and Law Enforcement Purposes

Derogations from the consent principle are allowed in limited circumstances, for example:

- To protect the health or safety of the individual or others (s. 40(1)).
- To a person carrying out an inspection, investigation or similar procedure that is authorized by a warrant or by law (s. 43(1)(g)).
- As required by law (s. 43(1)(h)).



Disclosure of Information Permitted in Emergency or other Urgent Circumstances

- Public Interest and Grave Hazards
- Health and Safety of an Individual/ Risk of Serious Harm to Person or Group
- Disclosures to Public Health Authorities
- Compassionate Circumstances
- Providing Health Care
- Liability protection



Number 7
July 2005

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

Fact Sheet

Disclosure of Information Permitted in Emergency or other Urgent Circumstances

Privacy legislation in Ontario does not prevent the rapid sharing of personal information in certain situations. While it is appropriate to recognize that personal information is protected by Ontario's privacy and access laws, it is also important to realize that these protections are not intended to stand in the way of the disclosure of vital – and in some cases, life-saving – information in emergency or other urgent situations.

In emergency and limited other situations, personal information, including personal health information, may need to be disclosed in a timely fashion, even if the person's consent has not been obtained. In such circumstances, the head of a public sector institution or a health information custodian (a defined term under the *Personal Health Information and Protection Act* or *PHIPA*), or those acting on their behalf, can – and in some cases must – disclose information that would normally be protected by Ontario's access to information and privacy laws. This information may be a record or

records containing personal information or personal health information, and the circumstances may include emergencies or critical situations affecting individuals or public health and safety, as well as situations calling for compassion.¹ Although these disclosures are the responsibility of the head of an institution or a health information custodian, it is important for anyone working in such settings to understand what is permitted in certain situations.

A head of a public sector institution or a health information custodian is given the authority by Ontario's access to information and privacy laws to disclose such information. These laws also protect a health information custodian or a head from damages, provided that the custodian or head has acted in good faith.

Listed below are some circumstances under which a custodian can disclose personal information or personal health information, in the absence of an individual's consent.

¹ "Head" and "personal information" are defined terms under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). "Health information custodian" and "personal health information" are defined in the *Personal Health Information Protection Act* (PHIPA). Please see <http://www.o-laws.gov.on.ca/>.



Raising Awareness about the Discretion to Disclose

- *“ I well appreciate that the decision to disclose sensitive health information without consent is an extremely difficult one to make, requiring a sound judgment call. A great deal of deliberation and discretion must be exercised. Disclosure may only be contemplated in extreme situations involving a significant risk of harm to a student or another person(s). But disclosure is not prohibited – privacy laws do not prevent you from doing so.”*
- Letters have been sent to all the presidents of universities and colleges in Ontario;
- We have met with the CEO of the Council of Ontario Universities and will be meeting with the entire Council at their next meeting;
- In conjunction with our counterparts in B.C., we will be issuing a Fact Sheet directed at colleges and universities to clarify the role that privacy legislation may play when workers are deciding whether or not to disclose personal health information.



*Technology-Related
Orders
Under PHIPA*



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.



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.

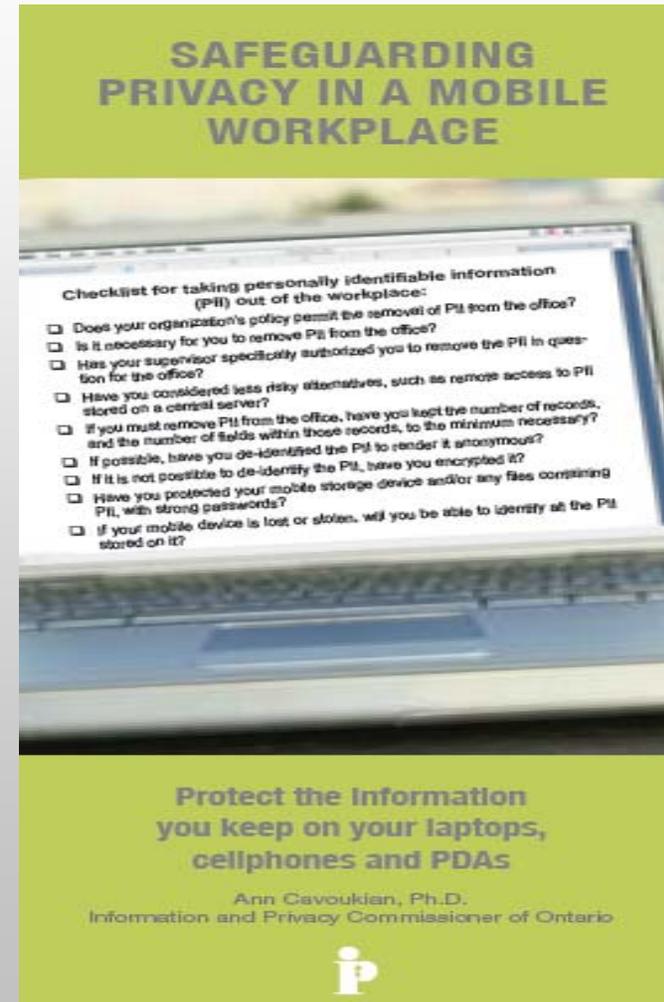
For example, "LetMeIn" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25"



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 issued two new Fact Sheets: *Wireless Communications Technologies: Video Surveillance Systems* and *Wireless Communication Technologies: Safeguarding Privacy & Security*.



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



*Electronic Health
Records (EHR)
in Ontario*



The Development of an EHR system in Ontario

Where are We?



Where Ontario Stands in the Development of EHR

Core systems in place by 2010:

- Registries
- Diagnostic imaging
- Public health surveillance system
- Client registry
- Provider registry
- Laboratory information system

Partially completed by 2010:

- Drug information system
- Diagnostic imaging system
- Interoperable electronic health record



Alternatives to Provincial EHR

I am exploring and comparing alternatives:

- **Sunnybrook MyChart** – A patient portal that allows the patient to view their personal health information (PHI) stored in Sunnybrook's electronic medical records;
- **HealthVault** – Internet-based product that allows patients to develop and control access to their own PHI. I have populated an account with my PHI from Sunnybrook and UHN;
- **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.



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.



Radio Frequency Identification (RFID)



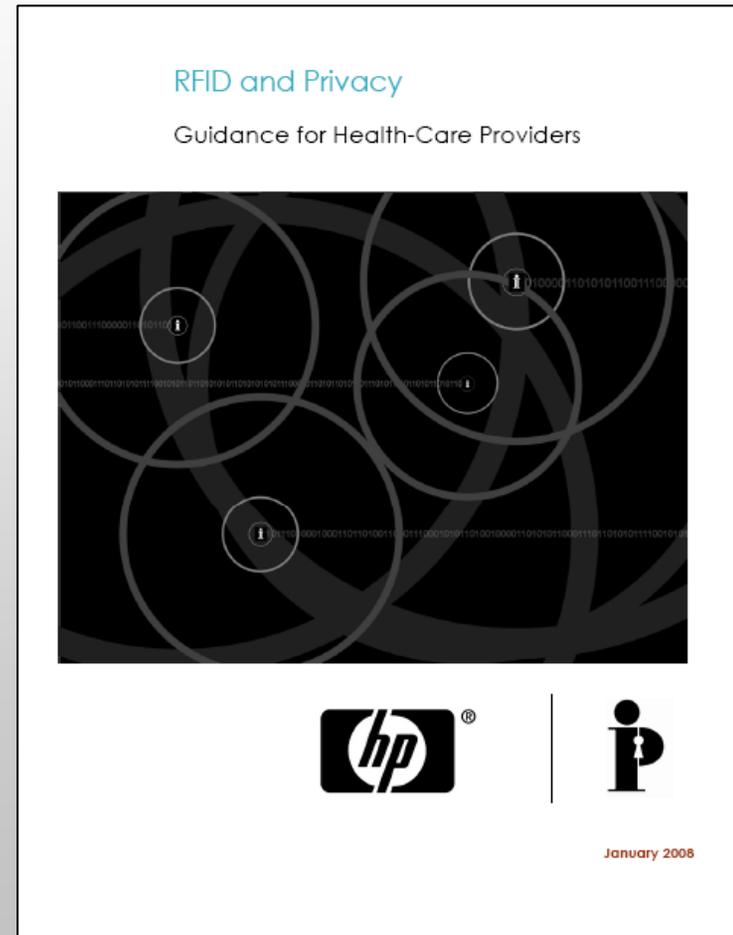
Why Privacy in RFID is Pivotal

- **Challenges when applying RFID technology in health care:**
 - RFID systems are a key part of an overall information system, so a **holistic systems approach** to privacy is warranted;
 - **RFID tags contain unique identifiers.** The ability to uniquely identify items has privacy implications when those items can be associated with identifiable individuals;
 - RFID tag data **can be read remotely**, without line-of-sight, without the knowledge or consent of the individual bearer. This has privacy implications for informed consent;
 - RFID data systems can also **capture time and location data**, upon which item histories and profiles may be constructed, making accountability for data use critical. When such systems are applied to identifiable individuals, it may invoke thoughts of surveillance.



RFID and Privacy in Health Care: *Guidance for Health Care Providers*

1. Tagging Things
2. Tagging Things Associated with People
3. Tagging People





Tagging Things

RFID technologies have proven to be ideal for identifying and locating things because they increase the reading accuracy and visibility of tagged items far beyond bar codes and other labels;

This can result in greater efficiency for automating inventory processes, finding misplaced items, and generally keeping better track of things as they move through their life-cycles;

Some RFID health care deployment scenarios that involve the tagging of things include:

- Bulk pharmaceuticals;
- Inventory and assets (trolleys, wheel chairs, medical supplies);
- Medical equipment and instruments (infusion pumps);
- Electronic IT devices (computers, printers, PDAs);
- Surgical parts (prosthetics, sponges);
- Books, documents, dossiers and files;
- Waste and bio-hazard materials.



Tagging Things Associated with People

RFID technology can involve tagging items that may be linked to identifiable individuals and to personal information, usually on a more prolonged basis – ranging from one week in the case of tagged garments, to several years in the case of patient dossiers.

Some examples of RFID deployment scenarios that involve tagging *things associated with people* include:

- Readers, tablets, mobile and other IT devices assigned to staff;
- Access cards assigned to staff or visitors;
- “Smart” cabinets
- Equipment, garments, or spaces (rooms) assigned to patients;
- Blood samples and other patient specimens;
- Patient files and dossiers; and
- Individual prescription vials.



Tagging People

RFID use can also involve the intentional tagging and identification of individuals. The distinction can be subtle since, technically speaking, it is always the tag that is identified in any RFID system.

When we talk about tagging people, we are focusing on the primary purpose of the RFID deployment in question, as well as the relative strength and permanence of the linkage of the tag to the individual and their personal information.

Examples of RFID used (or intended to be used) to identify and track individuals in health care contexts include:

- Health care employee identification cards;
- Patient health care identification cards;
- Ankle and wrist identification bracelets (patients, babies, Alzheimer's patients);
- Implantable RFID chips and other biosensors.



Applying RFID to Health Care

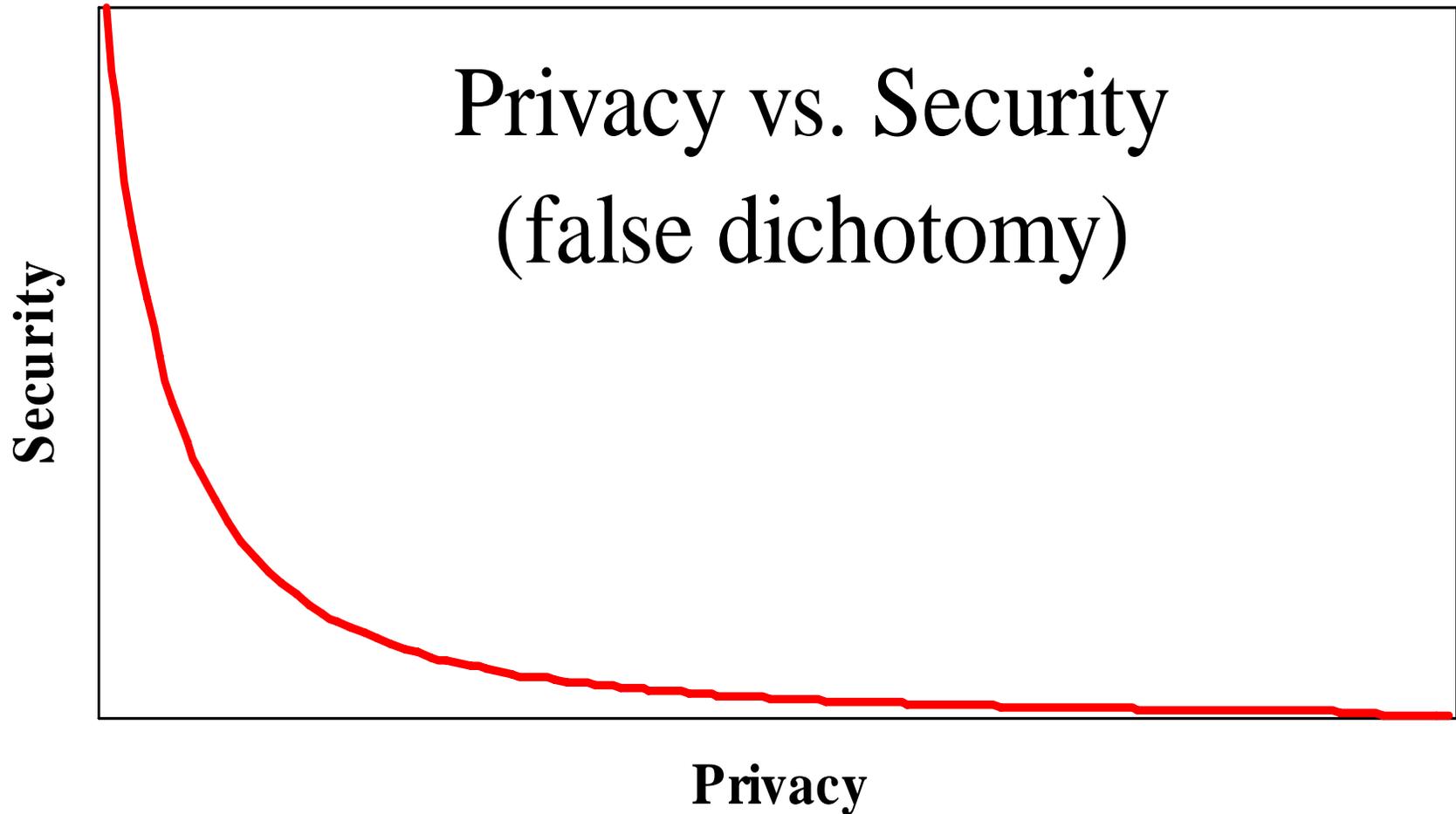




*Think “Positive-Sum”
not “Zero-Sum”*



Privacy OR Security: *A Zero-Sum Game*





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 trade-offs*



Looking at Privacy Differently

Old World: Zero-sum mentality

Future: Positive-sum paradigm

Don't get stuck in the past



Conclusions

- Privacy legislation does NOT pose a barrier to the disclosure of PHI in emergency or other urgent circumstances;
- Many high profile privacy breaches have resulted from the improper implementation or use of information technology;
- New technologies can pose a threat to privacy unless privacy is built into their design and implementation – we call this “*privacy by design*;”
- When implementing new technology, a Privacy Impact Assessment (PIA) is an essential tool to ensure that threats to privacy are identified early on so that issues can be addressed up-front;
- Think “positive-sum” not “zero-sum.”



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