

# **Privacy in the Context of Social Media and New Communication Technology in the Health Sector**

**Debra Grant, Ph.D.**

**Office of the Information and Privacy Commissioner of Ontario**

***CRTO Annual Education Day***

***December 2, 2011***

***Toronto***

[www.privacybydesign.ca](http://www.privacybydesign.ca)

## **Presentation Outline**

- 1. Protecting Personal health information***
- 2. Hot Topics***
- 3. Privacy by Design***
- 4. Costs of Privacy Breaches***
- 5. Conclusions***
- 6. Key Tips***

# Role of the Information and Privacy Commissioner of Ontario

- The Information and Privacy Commissioner (IPC) has oversight responsibility for three pieces of access and privacy legislation, including Ontario's health sector privacy legislation, the *Personal Health Information Protection Act (PHIPA)*
- This includes:
  - Public and stakeholder education
  - Providing information to the public on the legislation and the roles and responsibilities of the IPC
  - Receiving and responding to complaints
  - Undertaking reviews and investigations
  - Issuing orders

## Scope of *PHIPA*

- Provides individuals with a right of access to their records of personal health information held by health information custodians, subject to limited exceptions
- Provides rules for the collection, use and disclosure of personal health information by health information custodians

# Definition of Personal Health Information

Defined as identifying information that:

- Relates to a person's physical or mental health
- Relates to the provision of health care to the person
- Identifies a person's health care provider
- Identifies the person's substitute decision maker
- Relates to payments or eligibility for health care
- Is the person's health number
- Relates to the donation of body parts or substances
- Is a plan of service under *Long-Term Care Act, 1994*

## Why is the Need to Protect Personal Health Information So Critical?

The need to protect personal health information has never been greater given the:

- Extreme sensitivity of personal health information
- Number of persons involved in the provision of health care
- Emphasis on information technology including electronic records of personal health information
- Need to use or disclose health information for secondary purposes seen to be in the public interest

## Security of Personal Health Information

- Must ensure records of personal health information are retained, transferred and disposed of securely
- Must take steps that are reasonable in the circumstances to ensure personal health information is protected against:
  - Theft, loss and unauthorized use or disclosure
  - Unauthorized copying, modification or disposal
- Must notify individuals at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized person

**HOT ISSUES....**

**New Health Information and  
Communications Technology**





## The Promise of EHRs

- Electronic health records can facilitate the provision of more efficient and effective health care thereby improving the quality of the health care provided
- Paper-based records may be incomplete because records are spread over a range of health care providers and may be difficult to read and locate
- Electronic health records can be readily accessed by all health care providers regardless of where they are located, are more complete and require less space and administrative resources to maintain

# The Peril of EHRs

- If privacy is not built into the design, these systems pose unique risks to the privacy of individuals and to the security of personal health information
- These systems allow for the collection, use and disclosure of massive amounts of personal health information from diverse sources at the press of a key
- May attract hackers and others with malicious intent, including authorized health care providers who access the information for purposes other than providing health care
- Many high profile privacy and security breaches have resulted from inadequate safeguards for electronic records

## Is Digitized Data Riskier?

- Electronic records are not inherently riskier than paper-based records – the risks are different and must be managed differently;
- The features that make electronic records desirable for enhancing health care, also make them risky from a privacy perspective – enhanced accessibility, transferability and portability;
- Important to note that there is also the potential for stronger safeguards with electronic records (e.g., encryption, access controls, audit logs).

# The Perils of Paper-based Records: *Improper Disposal Results in Order*

- The Toronto Star ran a story describing the incident, along with a picture of the film set littered with what would appear to be patient records;
- A close-up of one patient record from an X-ray and ultrasound clinic also appeared with the story
- The patient's name was removed from the photograph of the actual health record.

## Film shoot uses real medical records

Privacy official has plans to investigate

RAJU MUDHAR  
STAFF REPORTER

A TV miniseries filming in downtown Toronto may have to answer to Ontario's privacy commissioner after it was discovered that "fake garbage" used in the movie actually consisted of patients' medical records from a Bathurst St. clinic.

The paper littered the sidewalk on Wellington St. W., near York St., yesterday for filming of *The Untold History of 9/11*, a Touchstone Television production about the Sept. 11, 2001, terrorist attacks on the United States that will air on ABC. Toronto is filming in for New York City, and fire trucks, police cruisers and stream garbage are being used to recreate the scene.

But much of the garbage yesterday was actually medical documents — mostly information about X-rays bearing the address of a Bathurst St. clinic. The material, noticed by someone on the movie set, included information about ultrasounds, chest X-rays and even diagnos-



TONY ROCK/TORONTO STAR

Mounds of medical records strewn along Wellington St. W. yesterday during filming of a TV miniseries on the 9/11 attacks. Below, an ultrasound report picked from the pile.

# Accessibility

- With electronic health records, more providers will have access to more information about more individuals than ever before (role-based access);
- Health care practitioners may be able to access more information than the patient might be able to provide a paper-based world;
- High profile breaches have resulted when someone with legitimate access abuses this right by improperly accessing information about someone they know, or a VIP out of curiosity (e.g., Ottawa hospital);
- Risk of unauthorized access can be managed through education, agreements, monitoring audit logs, and significant consequences for unauthorized access;
- Remote access increases external threats from hackers and others with malicious intent;
- There is no such thing as 100 per cent security – safeguards must continuously evolve to address emerging threats.

# Transferability

- Once information is digitized it is easy to transfer to portable devices (i.e., laptops, USB Keys, mobile devices) and remove from a secure facility or transfer to another health care provider, with the press of a key;
- The wrong information could be intentionally or inadvertently transferred to the wrong person.

# Portability

- Massive amounts of personal health information may be stored on a USB stick – privacy breaches are likely to be more catastrophic;
- Easy to take massive amounts of personal health information out of secure facility to work on at home;
- Portable computing and storage devices can be easily lost or stolen – they are often targets for thieves;
- This risk can be addressed by implementing data minimization whenever personal health information is transferred to a portable device and through the use of strong passwords and encryption;
- Must have strict policies regarding what information may be transferred to a portable device; any identifiable health information stored on portable devices must be encrypted.

# Wireless Communication Technology


## Order HO-005

- Received a report that a wireless mobile rear-assist parking device captured the image of an individual providing a urine sample at a methadone clinic
- The methadone clinic installed a wireless surveillance camera to monitor individuals providing urine samples
- Images are not recorded, images are only monitored in real time by a nurse working at the methadone clinic
- Consent is obtained for use of surveillance cameras



# Lessons Learned From Order HO-005

- Wireless surveillance cameras should not be used to transmit personally identifiable information without strong security and privacy precautions
- Should not conduct covert surveillance
- Health information custodians should:
  - Conduct privacy impact assessments and annual security and privacy audits
  - Ensure privacy and security requirements are explicit in the procurement process
  - Ensure the vendor selection process requires signal protection
  - Ensure the surveillance camera is off except when used for designated purposes
  - Post visible signs to advise patients of the existence of the surveillance cameras



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.

# E-mail Risks

## Disclosures of Personal Health Information:

- Sending the document to the wrong email address (e.g., email address is automatically filled in).
- Email sent to multiple individuals instead of blind copying to protect email addresses and individual identities.
- Document sent to the correct email address but viewed by an unintended recipient.
- The emailed document is forwarded to other individuals who do not need to know the information.
- The email address of the intended recipient has changed or the intended recipient is no longer using the email address.

## E-mail Benefits

- E-mail can also be helpful!
  - Scheduling
  - Patient reporting
  - Follow-up advice
  - Informative links
- Must ensure proper safeguards are in place, including secure e-mail and encryption.

## E-mail Considerations

- Regular email is not a secure means of communication and may be vulnerable to interception by unauthorized third parties.
- Unless physicians have access to a secure e-mail service offering strong encryption, they should avoid using e-mail to communicate personal health information.
- The e-mail service must meet *PHIPA* requirements, including security requirements and patients should have knowledge, consent and control over e-mail use.
- Even if patients may be willing to accept the risks associated with communicating with their physician via e-mail, this does not alleviate physicians of their duty to take steps that are reasonable in the circumstances to safeguard personal health information in their custody and control.

## Social Media (Facebook, Twitter, etc.)

- Health care providers may breach their duty to protect patient confidentiality and privacy
- Password protected sites may give users a false sense of security that they're in an exclusive environment.
- Loss of control over the information you share online.
  - Who's operating the platform and what are they able to see?
  - Do Facebook, Google or Twitter view, analyze or archive your communications on their platform?
- Even where information posted about patients may appear to be de-identified, others may be able to identify the patient through other information

## Workplace Blogging

- Blogs may be a great tool for education and collaboration in the workplace, but may pose a threat to patient privacy in health care settings.
- Online discussions pertaining to unusual medical conditions or patients with unique characteristics (e.g., an unusual occupation) may result in identifying patients and/or inadvertent disclosure of personal health information.

# Personal Health Records

- E.g., Microsoft Health Vault, Telus Health Space, Walmart, USB and smartphone applications
- Allows patients to integrate their own personal health information
- Can help patients to manage their own health care
- Allow patients to provide health care providers with access
- Unless these are directly link to EMRs, lack of interoperability results in information having to be inputted manually

# Patient Portals

- Can provide educational resources about diseases and conditions
- Can provide information about health care services provided
- Can provide individual with access to their own personal health information
- Can provide tools to help patients track and manage their own health and wellbeing
- Can allow patients to interact with their health care providers directly (e.g., appointment scheduling)



# Privacy Risks PHRs and Portals

- PHR users must ensure the privacy and security of their own information (e.g., strong passwords, firewalls, antivirus protection)
- User agreements may be complex and may lack transparency
- Patients can provide access to third parties
- Third party service providers could access the information for unintended purposes
- Third party service providers may not be bound by standards equivalent to health professional standards and may fall outside the scope of health privacy legislation

# Mobile Devices in Health Care

- Mobile applications are revolutionizing health care;
- Server-based applications designed to run on smartphones and tablets are allowing providers to access PHI at little cost, at any time, and from any location, and to share this information with others around the world;
- Mobile applications will bring health care to remote locations, avert medical emergencies, reduce hospitalization, and save lives.

# Examples of Smart Phone Applications

- A smartphone radiology product, developed by a Calgary-based company, has been approved for primary diagnostic use in Canada;
- In a UHN trial, at-home heart failure patients received handheld electrocardiogram devices that fed data to a smartphone which sent it to the hospital, where it was monitored by an algorithm that alerted a cardiologist if necessary;
- A smartphone application is being used in the U.S. to provide patients with direct access to laboratory test results;
- A smartphone application is being used in California to recruit citizens trained in CPR to provide emergency care to cardiac arrest victims nearby.

A large, light blue, stylized eye graphic is centered on the page. Inside the eye, the letters 'PbD' are written in a large, pink, serif font. The 'P' and 'D' are tall, while the 'b' is smaller and positioned between them. The background of the slide is a solid light blue color.

***Building Privacy into the  
Design of e-Health***

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# **Privacy by Design: The Trilogy of Applications**



**Information  
Technology**

**Accountable  
Business Practices**

**Physical Design  
& Infrastructure**

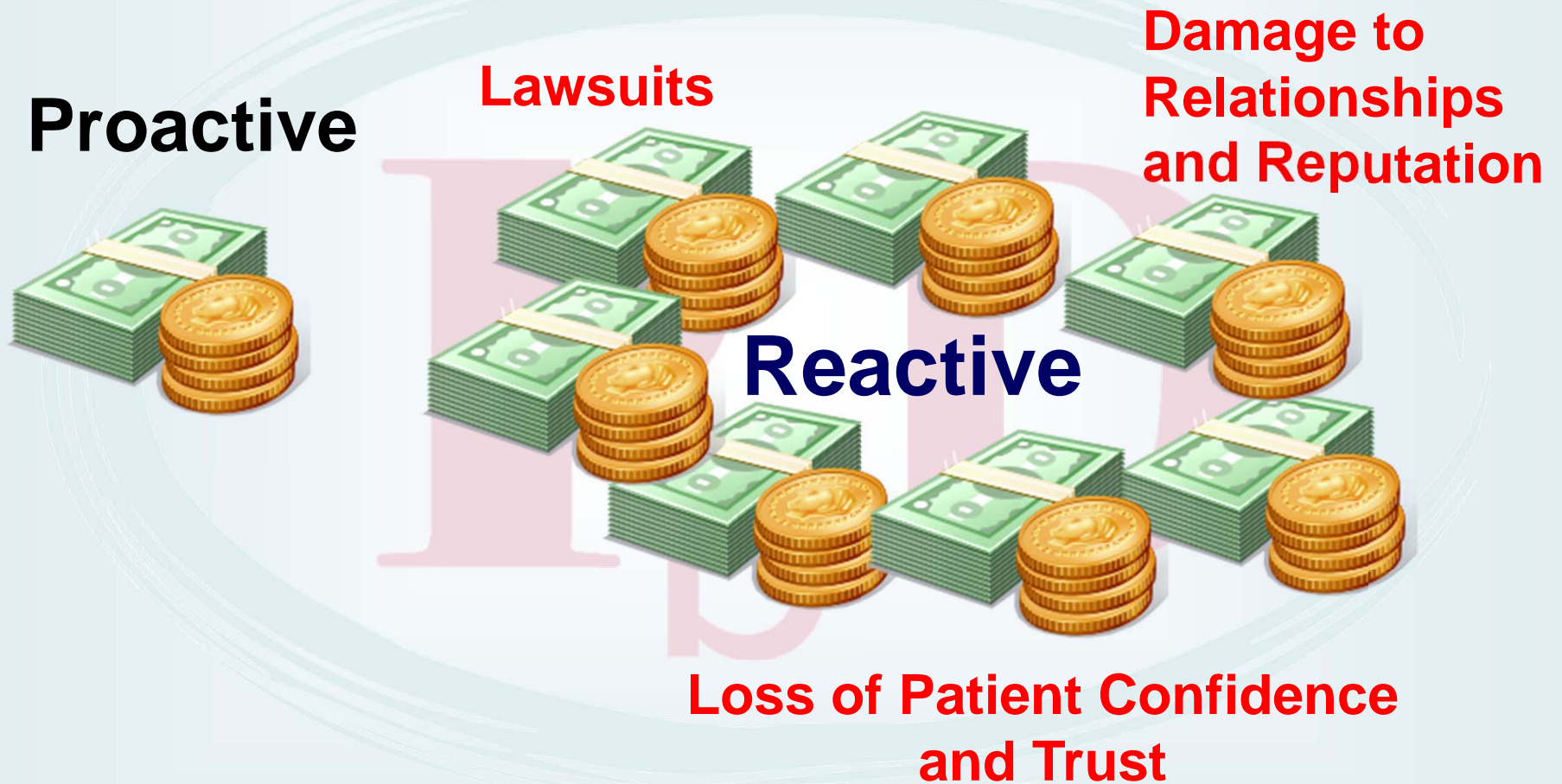
# Privacy by Design: “Build It In”

- The term “Privacy by Design” in the ‘90s, as a response to the growing threats to online privacy that were beginning to emerge;
- “Privacy by Design” seeks to build in privacy – up front, right into the design specifications; into the architecture; embed privacy into the technology used – *bake it in*;
- 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.

## Privacy by Design Will Help You Avoid

- Potential harm to individuals, including discrimination, stigmatization and economic or psychological harm
- Loss of trust or confidence in e-health by individuals and the health sector
- Damage to your reputation
- The time, expenses and resources necessary to contain, investigate and remediate privacy breaches
- The costs associated with legal liabilities and proceedings
- Potentially detrimental privacy protective behaviors, such as individuals not seeking treatment; withholding or providing false information and using multiple providers

# High Cost of Taking a Reactive Approach to Privacy Breaches





# Cost of Privacy Breaches in the U.S.

- A U.S. study found that between 2006/2007, over 1.5 million names were exposed during data breaches that occurred in hospitals.

— 2008 HIMSS Analytics Report: Security of Patient Data, Kroll Fraud Solutions

- Another U.S. study found that the cost of a data breach was \$202 per record; the average cost per operating company was more than \$6.6 million per breach.

— 2008 Annual Study: Cost of a Data Breach, Ponemon Institute

- Another U.S. report found that the average time it takes to restore an organization's reputation is one year and that the minimum brand damage was a 12% loss, increasing to nearly 25% in some instances.

— 2011 Survey, Ponemon Institute, February 2011

## Cost of Privacy Breaches in Ontario

*“Our experience indicates that breach management costs between \$100 and \$200 per individual, but this does not consider the cost to our reputation and the erosion of trust.”*

— Jacqueline Malonda, et al,  
Health Care Quarterly, Vol.12, No. 1, 2009.

# Costs of Legal Liability and Proceedings

- In December 2009, a public health nurse lost a USB key containing the unencrypted health information of 83,524 individuals attending an H1N1 immunization clinic
- Following my order in January 2010, a \$40 million class action was commenced by individuals affected by the breach
- This year the U.S. Department of Health and Human Services issued a number of fines for violating the *Health Insurance Portability and Accountability Act*, including a fine of \$4.3 million for failing to provide access and a fine of close to \$1 million for improper access to an EMR
- Additional proceedings are expected as the health sector moves toward electronic records and the public becomes increasingly concerned about what appears to be an epidemic of breaches

# Building A Culture of Privacy

- The commitment to privacy must come from the top down
- Think of privacy as a means of building trust and enhancing reputation rather than as a matter of compliance
- Integrate privacy into all programs and operations – never trade off privacy to achieve other important goals
- Devote adequate resources to the privacy program
- Ensure policies and procedures for maintaining privacy are clearly articulated and individuals know how to apply these policies and procedures in their day-to-day work

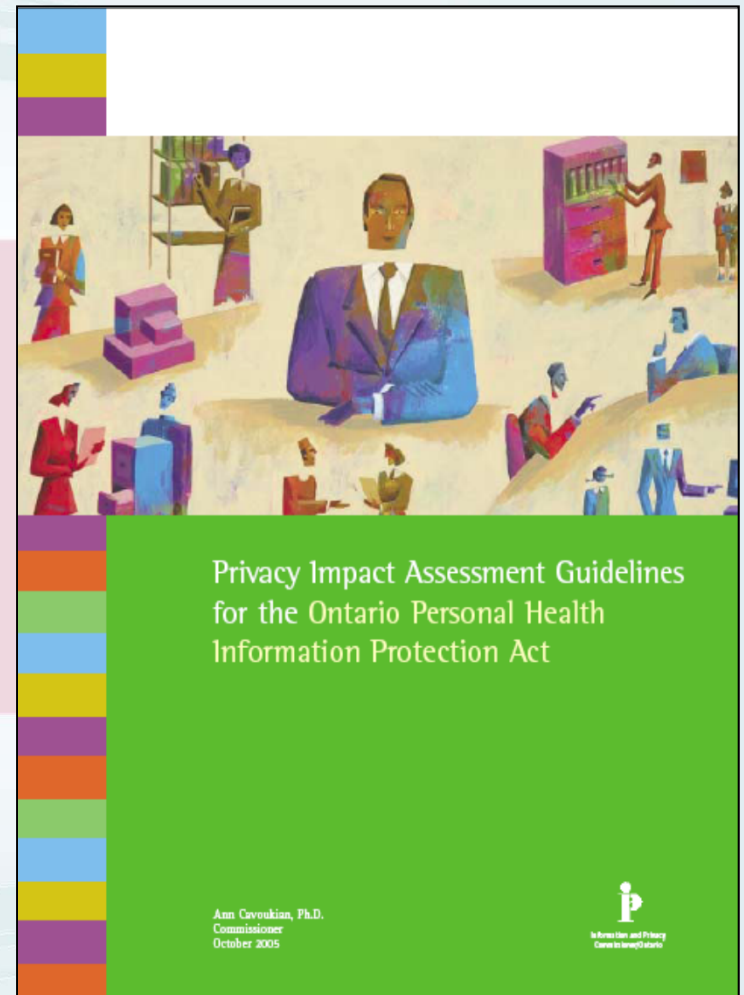
# Building A Culture of Privacy

- Provide on-going privacy and security training
- Use multiple means to communicate privacy messages
- Measure the effectiveness of your privacy program
- Make privacy a performance objective and performance standard for all individuals having an employment, contractual or other relationship with eHealth Ontario
- Build privacy into contracts with all service providers
- Conduct PIAs on proposed information systems, technologies and programs involving personal health information
- Plan for a privacy disaster by implementing a privacy breach management procedure

# Conduct Privacy Impact Assessments

The purpose of a privacy impact assessment is to:

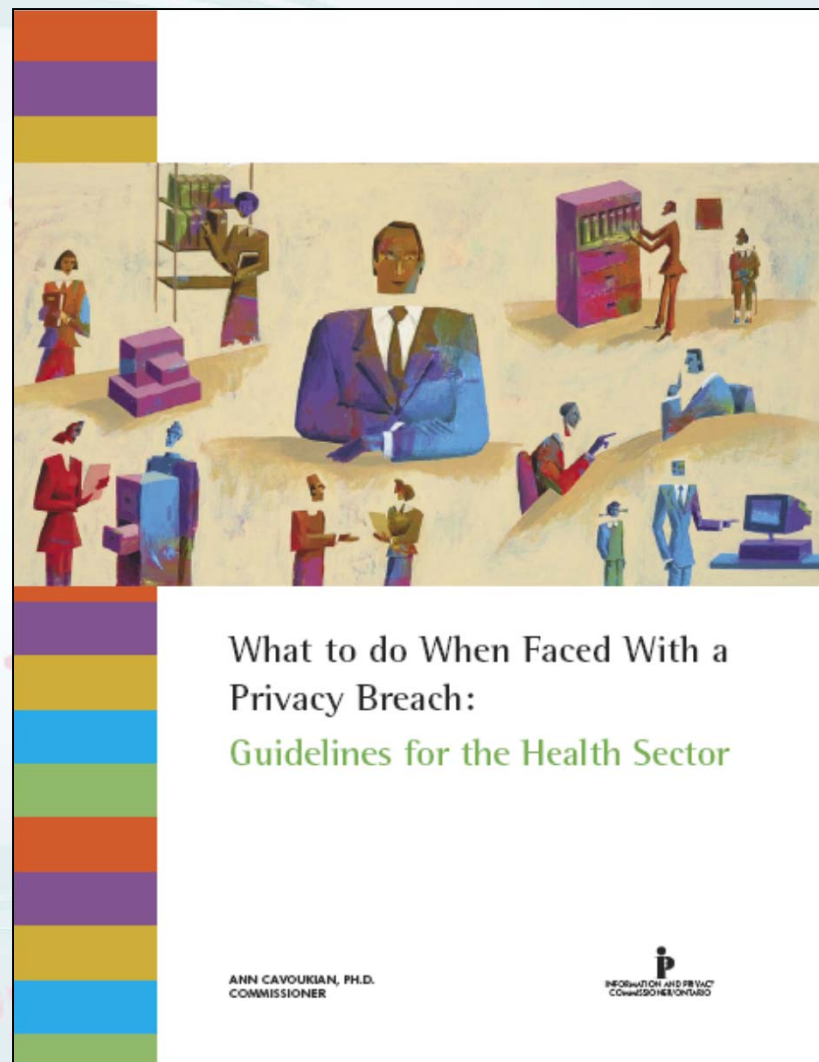
- Review the impact an information system, technology or program has on privacy
- Identify, address and mitigate actual or potential risks to the privacy of individuals
- Ensure the contemplated retention, collection, use, disclosure and disposal of personal information complies with relevant privacy statutes
- Ensure steps that are reasonable in the circumstances are taken to protect personal information from unauthorized use or disclosure
- Ensure personal information is retained, transferred and disposed securely



# Develop and Implement A Privacy Breach Management Procedure

The policy and procedure should

- Require employees to notify of a privacy or suspected privacy breach
- Identify who must be notified
- Clarify roles and responsibilities in responding to a privacy breach
- Outline the person responsible and the procedure to be followed in containing and investigating the privacy breach
- Identify the person responsible and the procedure to be followed in notifying individuals and senior management of the privacy breach



## Conclusion

- The same features of electronic health records that make them desirable from a health care perspective also make them challenging from a privacy and security perspective – accessibility, transferability and portability
- The risks can be managed by applying the principles of privacy by design
- If the risks are not managed, an epidemic of breaches in the context of new technology could set back the entire ehealth agenda
- It is easier and more cost effective to build in privacy upfront than to retrofit systems after the fact



## Key Tips

- Conduct Privacy Impact Assessments
- Build in *Privacy by Design*
- Minimize the use of personal health information wherever possible
- Use of secure channels, strong encryption and strong passwords and ensuring patients have knowledge, consent and control over the use of their personal health information
- Transparency and accountability is essential

# How to Contact Us

**Debra Grant, Ph.D.**

**Senior Health Privacy Specialist**

**Office of the Information & 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](http://www.ipc.on.ca)**

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

[www.privacybydesign.ca](http://www.privacybydesign.ca)