

Privacy *AND* Healthcare: You Need Both

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario, Canada**

**Joint Department of Medical Imaging
Mount Sinai / UHN/ Women's College Hospital
*September 22, 2011***

Presentation Outline

- 1. Ontario's Experience with PHIPA*
- 2. Circle of Care – Absolutely Essential*
- 3. Application of FIPPA to Hospitals*
- 4. Why Freedom of Information Matters*
- 5. FIPPA Complements PHIPA*
- 6. Preventing Privacy Breaches*
- 7. Conclusions*



*Ontario's Experience
with PHIPA*

www.privacybydesign.ca

Personal Health Information Protection Act (PHIPA)

- *PHIPA* came into effect on November 1, 2004;
- Provides comprehensive privacy protections for personal health information;
- Covers Health Information Custodians (HICs):
 - Hospitals;
 - Pharmacies;
 - Doctors, nurses and other health professionals;
 - Laboratories;
 - Agents of HIC's and recipients;
- *PHIPA* is a privacy statute that provides patients with a right of access to their health information and a right to complain to the IPC.

Implementing *PHIPA* in Ontario

- When *PHIPA* was first introduced in 2004, there was great concern about its impact on health care, especially among hospitals;
- My office was committed to working with the public, our government and health care sector, to ensure a smooth transition;
- Through appropriate planning, education and outreach, the legislation *did not pose any obstacles to the delivery of efficient and effective health care* in Ontario – implementation was surprisingly smooth;
- Health Information Custodians (HICs) did an excellent job cooperating with IPC in resolving issues – relatively few complaints to the IPC, with most being handled effectively by the HICs themselves;
- A review in 2008 of *PHIPA* indicated that it is working very smoothly – business as usual, with extremely high support for the legislation.

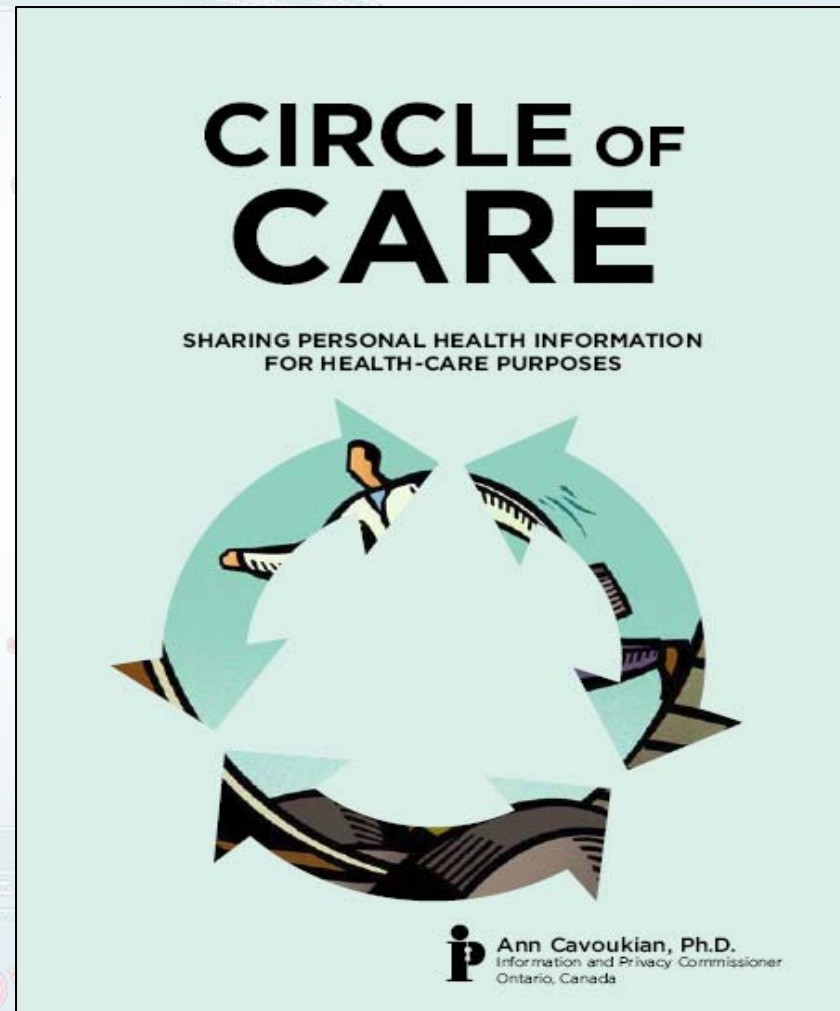
“Circle of Care”

Sharing Personal Health Information for Health Care Purposes

- The IPC issued a paper clarifying the circumstances in which a health information custodian may assume implied consent and the options available to a custodian where consent cannot be implied;
- While the term “Circle of Care” is not a defined term in *PHIPA*, it is invaluable;
- The term is commonly used to describe the ability of health information custodians to *assume* an individual’s *implied consent* to collect, use or disclose personal health information for the purpose of providing health care, in circumstances defined in *PHIPA*.

Circle of Care: Sharing Personal Health Information for Health Care Purposes

1. Health information custodian must fall within the a category of custodians that are entitled to rely on assume implied consent;
2. Information must have been received from the individual, his or her substitute decision maker or another custodian;
3. Information must have been received for the purpose of providing or assisting in the provision of health care to the individual;
4. Purpose of the collection, use and disclosure must be for providing health care or assisting in providing health care to the individual;
5. Disclosures must be to another custodian; *and*
6. Custodian must not be aware that the individual has expressly withheld or withdrawn consent to the collection, use or disclosure.





***Application of FOI
to Hospitals***

www.privacybydesign.ca

Why Freedom of Information Matters

Access + Transparency

=

Democracy

=

Freedom

*Transparency helps to create a culture
of openness and accountability*

A Culture of Openness

“As Premier, I believe the importance of the Freedom of Information and Protection of Privacy Act cannot be overstated...our government should ensure that information requested of it should continue to be made public unless there is a clear and compelling reason not to do so.”

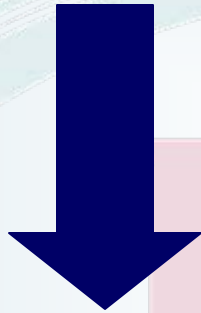
— Premier McGuinty, June 15, 2004

Application of *FIPPA* to Hospitals

- The *Broader Public Sector Accountability Act* received Royal Assent on December 8, 2010;
- This statute amends *FIPPA* to designate hospitals as institutions, effective January 1, 2012;
- *FIPPA* will apply to all records that came into the custody or control of a hospital on or after January 2007;
- A hospital is defined to include a public hospital, private hospital and the University of Ottawa Heart Institute.

FIPPA Complements PHIPA

FIPPA



*Public's Right
of Access to
General Records,
Not PHI*

PHIPA



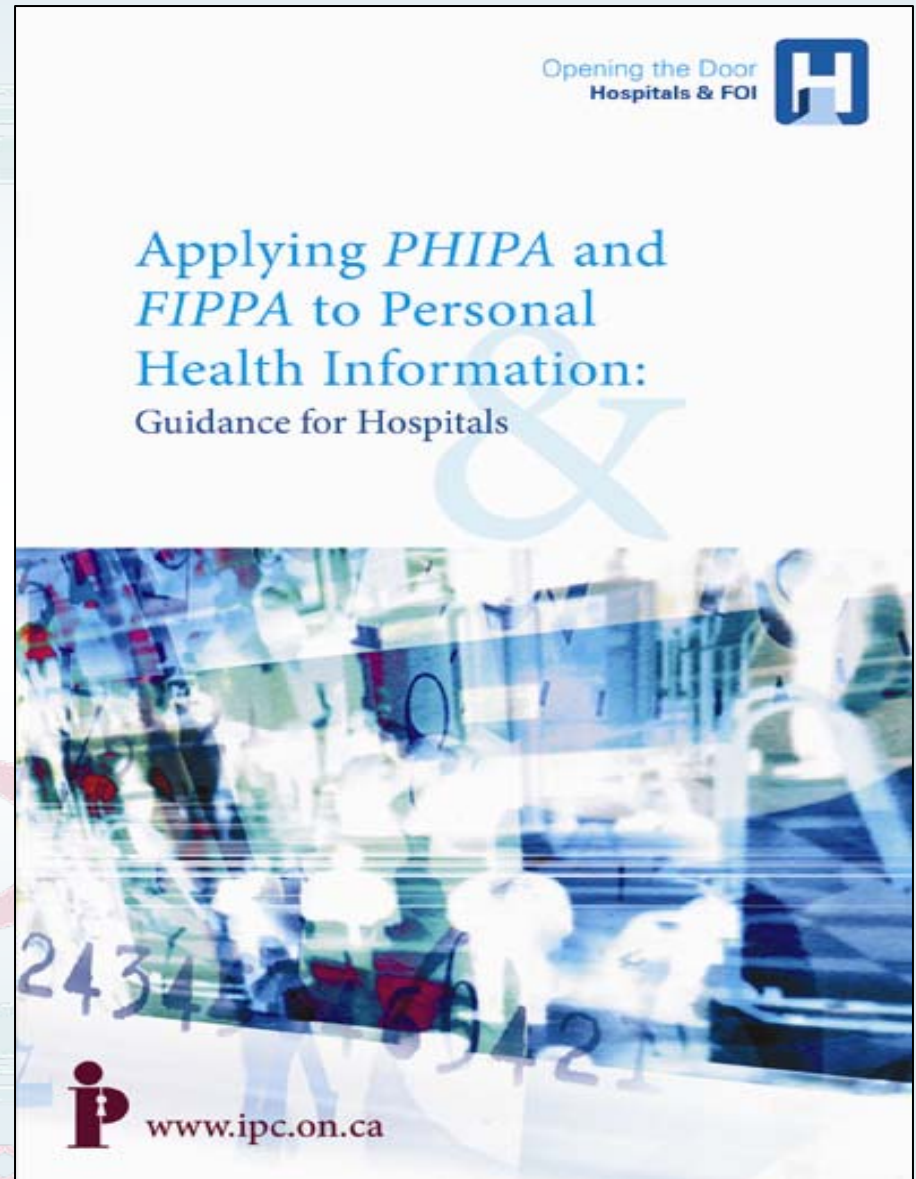
*Protection of
Personal Health
Information
(PHI)*

Hospital-Specific Provisions

- Rules to permit fundraising;
- Exemption for teaching materials;
- **Excluded from *FIPPA*:**
 - Certain Quality of Care information;
 - Ecclesiastical records;
 - Hospital foundation records;
 - Research data;
 - Records relating to appointments and privileges.

IPC Guidelines

- Required Disclosures;
- Permitted Disclosures;
- Mandatory Exemption from Disclosure;
- Discretionary Exemption from Disclosure;
- Access Rights;
- Permitted Collection;
- Permitted Use or Disclosure;
- Agent Information.





***Preventing
Privacy Breaches***

www.privacybydesign.ca

What Can Health Care Organizations Do to Ensure Privacy?

1. Create and implement a strong *Privacy Policy* – one that is in compliance with laws and regulations and has real consequences for privacy breaches;
2. Appoint a *Chief Privacy Officer* who is responsible for overseeing the privacy policy. The key here is accountability – responsibility for the privacy practices of your organization;
3. Develop an *Education and Training Program* for employees – make sure they understand what the privacy policy entails and are made aware of the laws and regulations that apply to their work;
4. Conduct a *Privacy Impact Assessment* (PIA) – a risk management tool used to identify the potential effects that an information system or technology may have on privacy.

What Can Individual Health Care Providers Do to Ensure Privacy?

- ***DO NOT*** discuss PHI in public places – (i.e., elevators, waiting rooms, etc.) or on social media (i.e., Facebook, chatrooms, Twitter or blogs);
- ***Only*** access PHI of patients to whom you are providing care;
- ***DO NOT*** leave records of PHI unattended – retain records in locked filing cabinets and locked offices;

What Can Individual Health Care Providers Do to Ensure Privacy? (Cont'd)

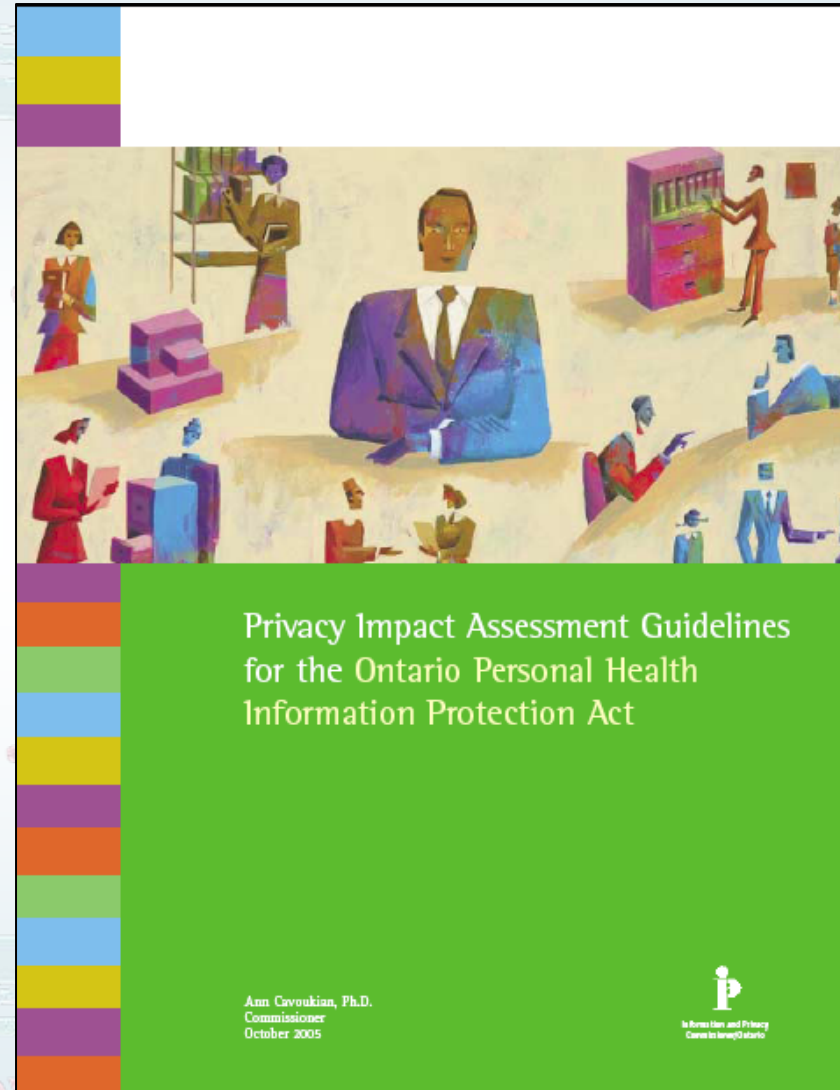
- ***DO NOT*** remove PHI from a secure work environment unless it is absolutely necessary and only if appropriate safeguards are implemented;
- When it is necessary to store PHI on mobile devices, ***make sure*** that the information is either de-identified or strongly encrypted, and that the device is protected with a strong password;
- ***Delete*** PHI from mobile devices when no longer needed;
- ***DO NOT*** write down or share your passwords;

What Can Individual Health Care Providers Do to Ensure Privacy? (Cont'd)

- When disposing of any PHI (paper or electronic) make sure that it is *securely destroyed* in accordance with your organization's prescribed methods – **DO NOT** throw it in the trash or standard recycling bin;
- **Notify your designated privacy officer** about any privacy breaches, suspected privacy breaches or practices that may result in breaches;
- **If in doubt** about *PHIPA* or privacy and health information, ask your designated privacy officer or call us, the IPC, at **1-800-387-0073 / 416-326-3333** – *we are here to help.*

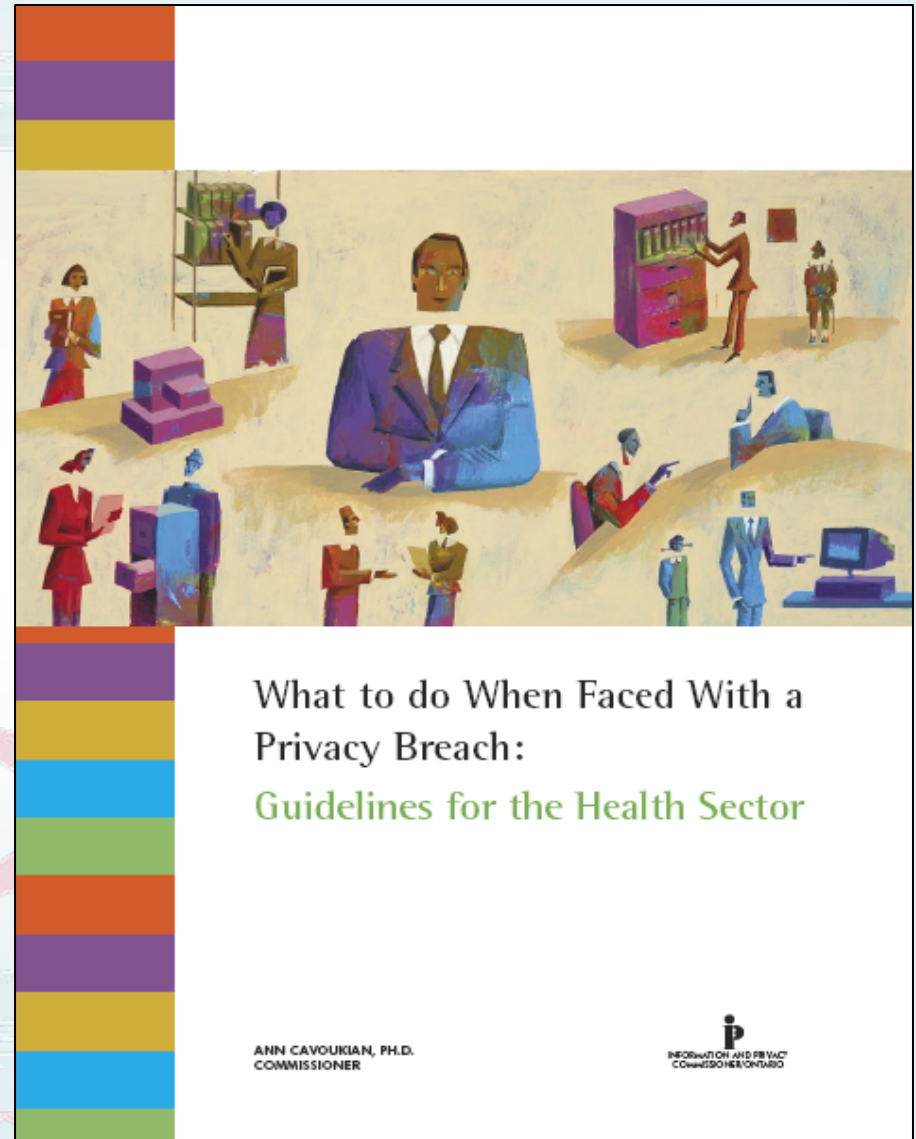
Privacy Impact Assessment (PIA)

- An assessment tool used to identify the risks that a proposed or existing technology or program may have on privacy;
- The IPC developed this publication as a self- assessment tool to assist health information custodians in reviewing ways in which privacy risks can be mitigated.



Implement A Privacy Breach Protocol

- Explains why you need a Privacy Breach Protocol;
- Covers steps including:
 - Respond immediately;
 - Contain the harm;
 - Notify patients;
 - Investigation and remediation.
- Tips to avoid breaches.



Health Orders Regarding Unencrypted Mobile Devices

- **HO-004** (2007) – A physician at SickKids Hospital had his *unencrypted laptop* stolen from his car containing the identifiable PHI of 2,900 patients involved in research studies;
- **HO-007** (2009) – A nurse lost an *unencrypted USB key* containing the PHI of nearly 84,000 people who had attended H1N1 immunization clinics in Durham Region;
- **HO-008** (2010) – A nurse had her *unencrypted laptop* stolen from her car containing 20,000 patient records with names, medical records, surgeries performed and physician information.

Stop. Think. Protect



... Protecting Personal Information on Mobile and Portable Devices



www

sign.ca

STP - STOP. THINK. PROTECT.

- 1. STOP** – Ask yourself: Do I really need to store any personal health information on this device?
- 2. THINK** – Consider the alternatives. Would de-identified or coded information serve the same purpose? Can you access the information remotely through a secure connection or virtual private network instead?
- 3. PROTECT** – If you must store personal health information on mobile devices it must be encrypted and protected with strong passwords. In addition, you must store the least amount of information possible, for the shortest amount of time.

Build 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 strong message that comes right from the top;
- One way of getting the message across is by devoting adequate resources to privacy initiatives and programs;
- Privacy must be directly inter-woven into the fabric of the day-to-day operations of a hospital or organization.



www.privacybydesign.ca

Privacy by Design

Access by Design



Access by Design

Conclusions

- Citizens need to have access to information to participate meaningfully in society; Patients need access to their own health records;
- Any exemptions from the right of access should be limited and specific;
- If implemented properly, the new *FIPPA* provisions will not impede hospital operations or the delivery of health care services – plan ahead, *be proactive!*
- Implement a Privacy Breach Protocol;
- Stop. Think. Protect;
- Develop a Culture of Privacy and weave it into the fabric of your hospital.

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) 326-3948 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

For more information on hospitals under *FIPPA* visit:

www.ipc.on.ca/english/Access-to-Information/For-the-Public/