

Protecting Privacy in an Era of Electronic Health Records

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario**

*Barrie and Community Family Health Team
Royal Victoria Hospital – Georgian College*

November 22, 2012

Outline of Presentation

- 1. Importance of Protecting Privacy in the Electronic Age*
- 2. The Promise and Peril of Electronic Health Records*
- 3. Consequences of Inadequate Attention to Privacy*
- 4. Three Major Risks:*
 - Privacy Risks During Transition*
 - Unauthorized Access to Electronic Records*
 - Mobile and Portable Devices*
- 5. Privacy by Design: The Gold Standard*
- 6. Building Privacy into the Design of Electronic Records*
- 7. Conclusions*



***Importance of Protecting
Personal Health Information***

www.privacybydesign.ca

Unique Characteristics of Personal Health Information

- Highly sensitive and personal in nature – in need of strong protection;
- But must be shared immediately among a range of health care providers, for the benefit of the patient;
- Also used and disclosed for secondary purposes seen to be in the public interest (e.g., research, health system planning and evaluation, quality assurance);
- This dual nature of personal health information is reflected in *PHIPA*.

Why Protecting Personal Health Information is So Critical

- Extreme sensitivity of personal health information;
- Massive growth in online connectivity;
- Increasing number of persons involved in the delivery of health care;
- Emphasis on information technology, including electronic medical records and electronic health records;
- Health information forms the basis of invaluable research, seen to be in the public interest, but which could be jeopardized if the public's trust is eroded.



The Promise and Peril
of
Electronic Health Records

www.privacybydesign.ca

Definitions

- **Electronic Health Record:**
 - An electronic record that integrates information about the care and treatment provided to a patient by multiple health care providers;
- **Electronic Medical Record:**
 - An electronic record used by a health care provider that only includes information about the care and treatment provided to a patient by that one health care provider;
- **Personal Health Record:**
 - An application that allows patients to create, review, annotate or maintain a record in respect of their own care and treatment.

The Promise of Electronic Health Records

- Can facilitate the provision of more efficient and effective health care and improve the quality of care provided;
- Easier to read and locate than paper records;
- Require less space and fewer administrative resources to maintain;
- Can be designed to enhance privacy through access controls, audit logs, strong encryption and authentication;
- EHRs may be more complete and readily accessible by all health care providers involved in the health care of a patient, regardless of location.

The Peril of Electronic Health Records

- If privacy is not embedded in the design of EHRs, unique risks to privacy and the security of personal health information arise;
- Allows for massive amounts of personal health information from diverse sources to be collected, used and disclosed;
- Unauthorized uses attracts hackers and others with malicious intent, including authorized health care providers who access the information for purposes other than providing health care;
- Easier to transfer personal health information to a portable device and remove the information from a secure location.



***Consequences of Inadequate
Attention to Privacy***

www.privacybydesign.ca

Consequences if Inadequate Attention Paid to Privacy

- Individuals may be deterred from seeking testing or treatment, or may engage in multiple doctoring;
- Individuals may withhold or falsify information provided;
- Loss of trust or confidence in the health system;
- Damage to the reputation of the health care provider;
- Individuals may suffer discrimination, stigmatization and economic or psychological harm;
- Lost time and expenditure of resources needed to contain, investigate and remediate privacy breaches;
- Costs of legal liabilities and ensuing proceedings.

Three Major Privacy Risks:

- 1. Privacy Risks During Transition***
- 2. Unauthorized Access to Electronic Records***
- 3. Mobile and Portable Devices***

A large, light pink, semi-transparent logo consisting of the letters 'P', 'b', and 'D' in a stylized font, centered in the background. The 'P' and 'D' are tall and blocky, while the 'b' is smaller and lowercase. The entire logo is enclosed within a light green, double-lined oval border.

Privacy Risks
During Transition

www.privacybydesign.ca

Privacy Risks During the Transition to Electronic Records

Personal health information may be most vulnerable when transitioning to electronic records – why?

- Staff may not be fully trained on the new electronic system;
- The electronic system may not be fully functional;
- Privacy and security features may be turned off or set to minimal protection;
- Conversion of paper records to electronic format may require frequent access to the records by larger numbers of people;
- Records may be duplicated in paper and electronic format, thereby increasing the volume of records requiring protection.

A Practical Tool for Physicians Transitioning to Electronic Records

- My office jointly published a toolkit with Dr. Peter Rossos, at the University Health Network, for managing privacy issues during the transition to electronic records.
- The toolkit addresses:
 - Education and training of staff;
 - Implementation of access controls;
 - Implementation of strong passwords;
 - Audits of access to electronic records;
 - Managing the retention, transfer and disposal of paper records;
 - Drafting or updating privacy and security policies and procedures.

Personal Health Information:

A Practical Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Peter G. Rossos, MD, MBA,
FRCP(C), FACP
Chief Medical Information Officer
UHN & SIMS Partnership

May 21, 2009



***Unauthorized Access
to Electronic Records***

www.privacybydesign.ca

Your Medical Records May Not Be “Private”

- An ABC News investigation found medical records can be purchased online;
- With two clicks of a mouse, an IT specialist found someone willing to sell names, birthdates and insurance providers of patients with diabetes and someone willing to sell records of those who purchased health insurance in the last 3 to 12 months;
- Many of the breaches occur through theft or hacking, inadvertent loss and inside jobs – identity thieves may approach medical staff and offer up to \$500 a week for providing 20 insurance claim forms, medical records or health financing records;
- For example, in June, 2012, a technician at Howard University pleaded guilty to selling patient information, including names, birthdates and Medicare numbers, for \$500 to \$800 per transaction, for more than a year!

— *Your Medical Records May Not Be Private*,
ABC News Investigation, September 13, 2012,
<http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986>

Orders HO-002 and HO-010

The IPC has issued two orders involving unauthorized access to electronic records of personal health information:

Order HO-004 – A girlfriend of the patient’s estranged husband, who was a nurse at the hospital but who was not involved in the care of the patient, viewed the patient’s electronic record on numerous occasions;

Order HO-010 – A former spouse of the patient’s current spouse, who was a diagnostic imaging technologist at the hospital but who was not involved in the care of the patient, viewed the patient’s electronic records on multiple occasions.

Examples of Unauthorized Access in Other Jurisdictions

- In 2011, a pharmacist in Alberta was fined \$15,000 for accessing the information of 11 women who attended her church and posting prescription information on Facebook;
- In 2011, a physician in Alberta accessed the information of his partner's former spouse and the mother and girlfriend of the former spouse for a divorce and custody dispute;
- In 2012, a clerk at Western Health in Newfoundland is alleged to have accessed the information of over 1,000 individuals for unauthorized purposes;
- In 2012, Eastern Health in Newfoundland terminated five employees and suspended 6 others for unauthorized access.

Detering and Preventing Unauthorized Access to Electronic Records

- Immediately terminate access to the records pending an investigation into the issue of unauthorized access;
- Implement appropriate access controls;
- Consider the use of “VIP flags;”
- Log and audit access to records;
- Implement a policy of “zero tolerance” and impose appropriate discipline for unauthorized access;
- Provide training and raise awareness related to appropriate access, including through confidentiality agreements and reminder notices displayed on log in to electronic records.

A large, light pink, semi-transparent logo consisting of the letters 'P', 'b', and 'D' in a stylized font. The 'P' and 'D' are tall and blocky, while the 'b' is smaller and positioned between them. The logo is centered within a light blue oval frame that has a subtle gradient and a slight shadow effect.

Mobile and Portable Devices

www.privacybydesign.ca

Risks of Retaining Electronic Records on Mobile and Portable Devices

- My office has issued three orders involving mobile and portable devices in the health sector:

Order HO-004

- Theft of a laptop containing the unencrypted personal health information of 2,900 individuals

Order HO-007

- Loss of a USB memory stick containing the unencrypted personal health information of 83,524 individuals

Order HO-008

- Theft of a laptop containing the unencrypted personal health information of 20,000 individuals

Reducing the Risks Associated with Mobile and Portable Devices

- Do not transfer or store personal health information on mobile devices;
- Consider the alternatives, such as:
 - Retaining de-identified information on the device;
 - Retaining encoded information on the device and storing the code to unlock the identifying information separately on a secure computing device; or
 - Retaining personal health information on a secure server and accessing the information remotely through a secure connection or virtual private network.

STOP. THINK. PROTECT.

Patient Privacy is in Your Hands.



As health care practitioners, many of you are accustomed to dealing with loss. You interact with people every day who have lost their health, lost a loved one, or perhaps simply lost hope. And you are experts at helping people work through and manage that sense of loss.

But what if you, yourself, were responsible for the loss of something that a patient may never get back: their privacy?

Earlier this year, a health care professional did something seemingly well-intentioned: she placed a USB key into her purse as she left the office, planning to do some work at home. As it happened, the files in question were the records of personal health information of 763 patients.

Her purse was stolen. And all the records – unencrypted and easily read by anyone – were lost. Lost, too, was the sense of privacy of those 763 patients.

Scenarios such as this have been played out countless times all across Ontario. Indeed, in recent years, the unencrypted health information of over 100,000 patients on laptops, USB keys and other mobile computing and storage devices has been lost or stolen. It's a privacy problem of epic proportions, compromising some of the most sensitive and personal types of information possible. And it must stop.

The *Personal Health Information Protection Act* requires that you take reasonable steps to ensure that personal health information is protected against theft, loss, and unauthorized use and disclosure.

Mobile devices, such as laptops, PDAs, and USB keys, add a new layer of complexity to this task. The great advantage of these devices – portability – is also their greatest vulnerability, making them easily susceptible to loss and theft.

For that reason, personally identifiable health information should not be stored on any mobile devices unless it is absolutely necessary. And when it is, you can – and **must** – take steps to minimize the risks to privacy.

Reducing the Risks Associated with Mobile and Portable Devices *(Cont'd)*

- If you must retain personal health information on a mobile or portable device:
 - Strongly encrypt the personal health information;
 - Ensure the encryption keys are not stored with or on the device;
 - Ensure the use of strong password protection;
 - Only retain the minimal amount of information and for the minimal amount of time necessary;
- Develop a policy for secure retention on mobile devices:
 - Provide training on the policy and procedures;
 - Regularly audit compliance with the policy;
 - Regularly review the policy and procedures.

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.

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
- A U.S. report found that the average time it takes to restore an organization's reputation following a data breach is one year and that the minimum brand damage is a 12% loss.
 - 2011 Survey, Ponemon Institute, February 2011

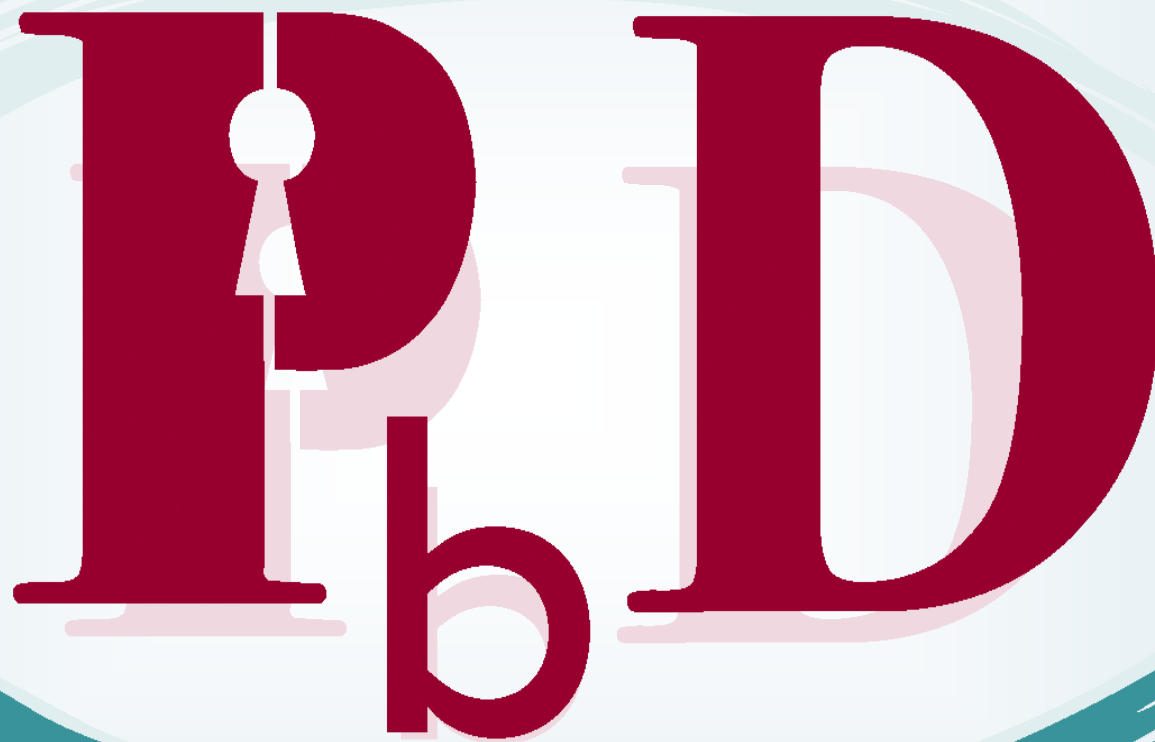
Costs of Legal Liabilities and Proceedings

- 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 initiated by individuals affected by the breach;
- A settlement was reached and approved by the Ontario Superior Court of Justice on July 12, 2012;
- Last year in the U.S., a number of fines were issued 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 electronic medical record.



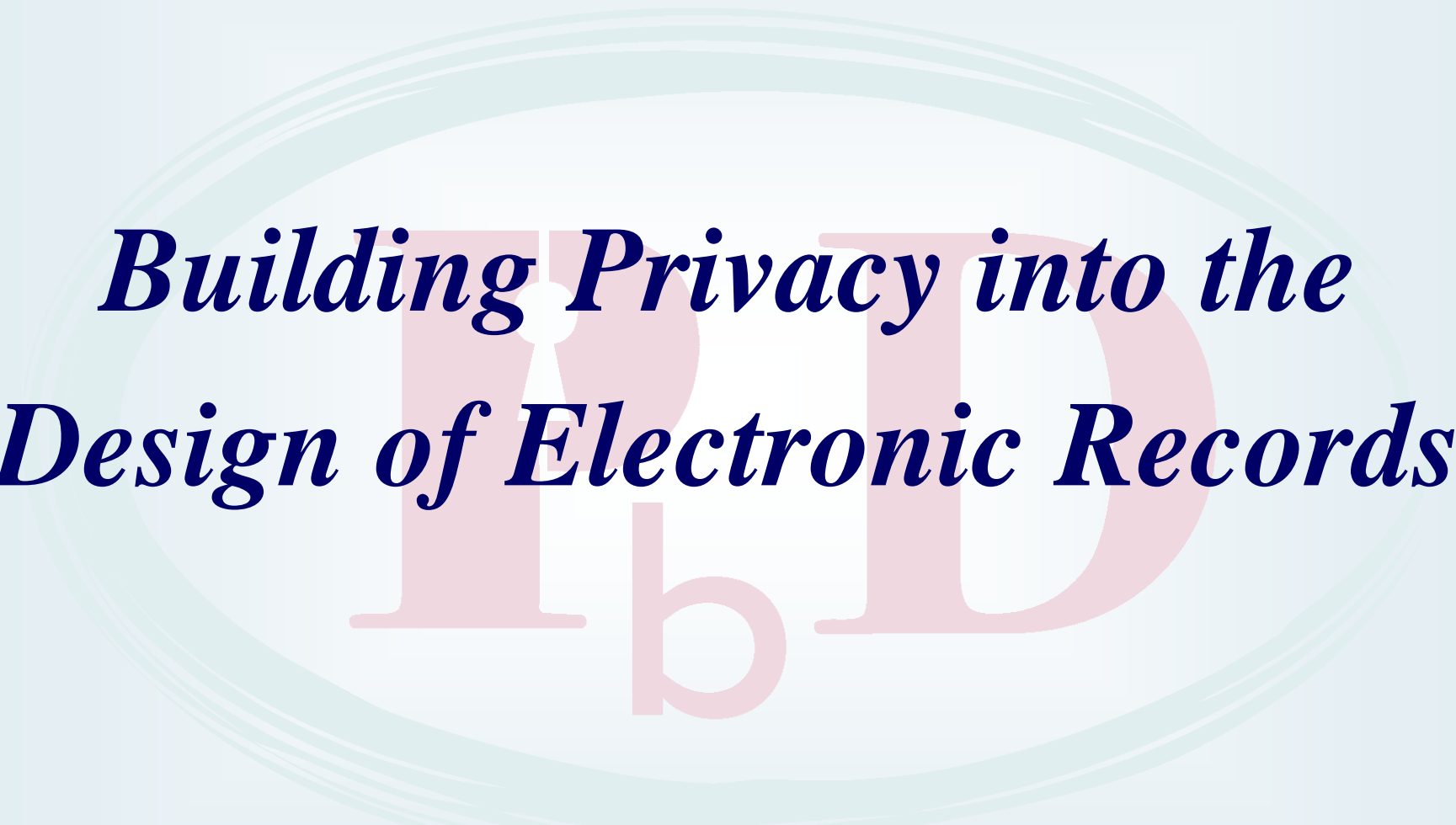
***Minimizing the Risk
of Privacy Breaches***

www.privacybydesign.ca



PbD

www.privacybydesign.ca



***Building Privacy into the
Design of Electronic Records***

www.privacybydesign.ca

Adoption of “Privacy by Design” as an International Standard

Landmark Resolution Passed to Preserve the Future of Privacy

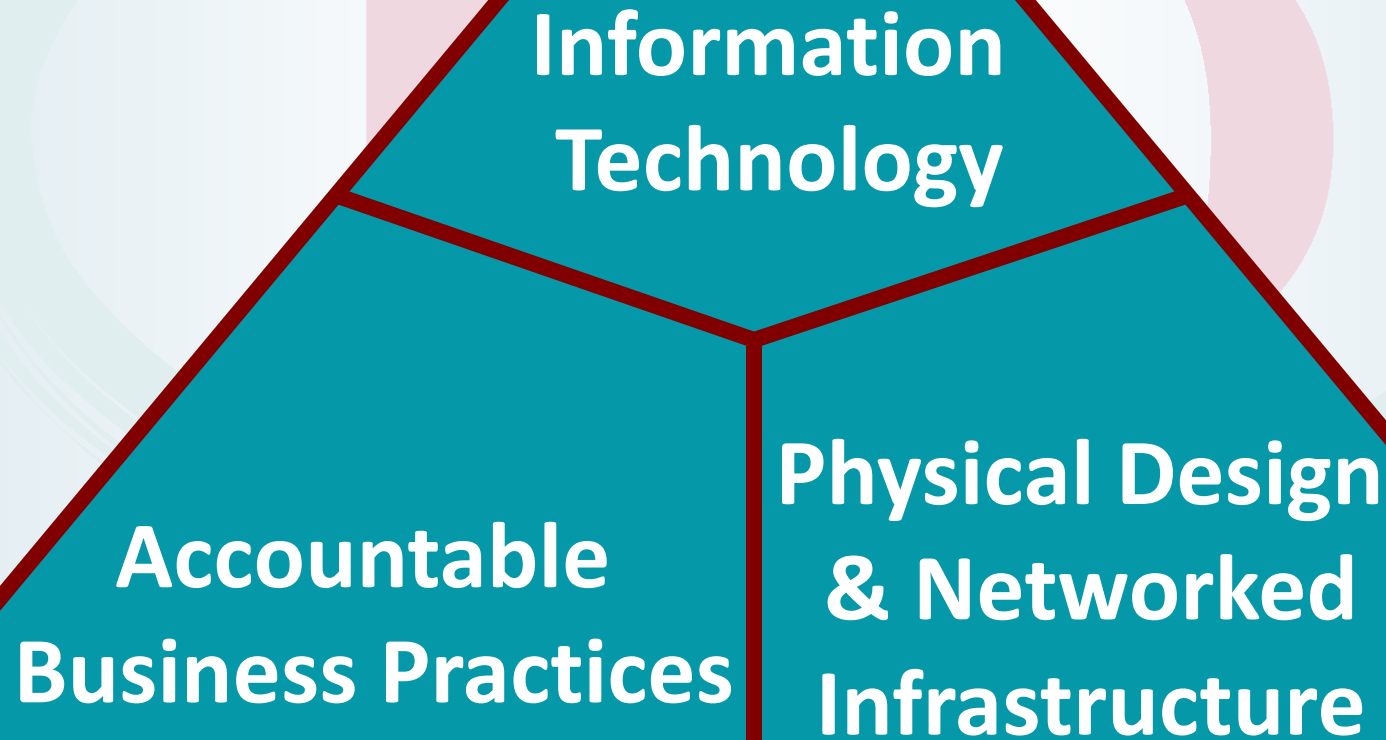
By Anna Ohlden – October 29th 2010 - http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

JERUSALEM, October 29, 2010 – A landmark Resolution by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, was unanimously passed by International Data Protection and Privacy Commissioners in Jerusalem today at their annual conference. The resolution ensures that privacy is embedded into new technologies and business practices, right from the outset – as an essential component of fundamental privacy protection.

Full Article:

http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

Privacy by Design: *The Trilogy of Applications*



Privacy by Design: *The 7 Foundational Principles*

1. ***Proactive*** not ***Reactive***:
Preventative, not Remedial;
2. Privacy as the ***Default*** setting;
3. Privacy ***Embedded*** into Design;
4. ***Full*** Functionality:
Positive-Sum, not Zero-Sum;
5. End-to-End ***Security***:
Full Lifecycle Protection;
6. Visibility and Transparency:
Keep it Open;
7. Respect for User Privacy:
Keep it User-Centric.



Privacy by Design
The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to *PETS Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in *PETS Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles (*see over page*):

Build A Culture of Privacy

- Build a culture of privacy – privacy must be built into the operational processes and practices of health care providers;
- The commitment to privacy must come from the top down;
- Think of privacy as a means of building trust rather than just a matter of regulatory compliance;
- Ensure those acting on your behalf know how to apply privacy policies and procedures in their day-to-day work;
- Provide on-going privacy and security training;
- Use multiple means to communicate privacy messages;
- Measure the effectiveness of your privacy program.

The logo for Privacy by Design is a light blue oval with a double-line border. Inside the oval, the letters 'P', 'b', and 'D' are arranged in a stylized, light red font. The 'P' and 'D' are large and blocky, while the 'b' is smaller and lowercase, positioned between them. The text 'Data Minimization' is written in a dark blue, italicized serif font across the middle of the oval.

Data Minimization

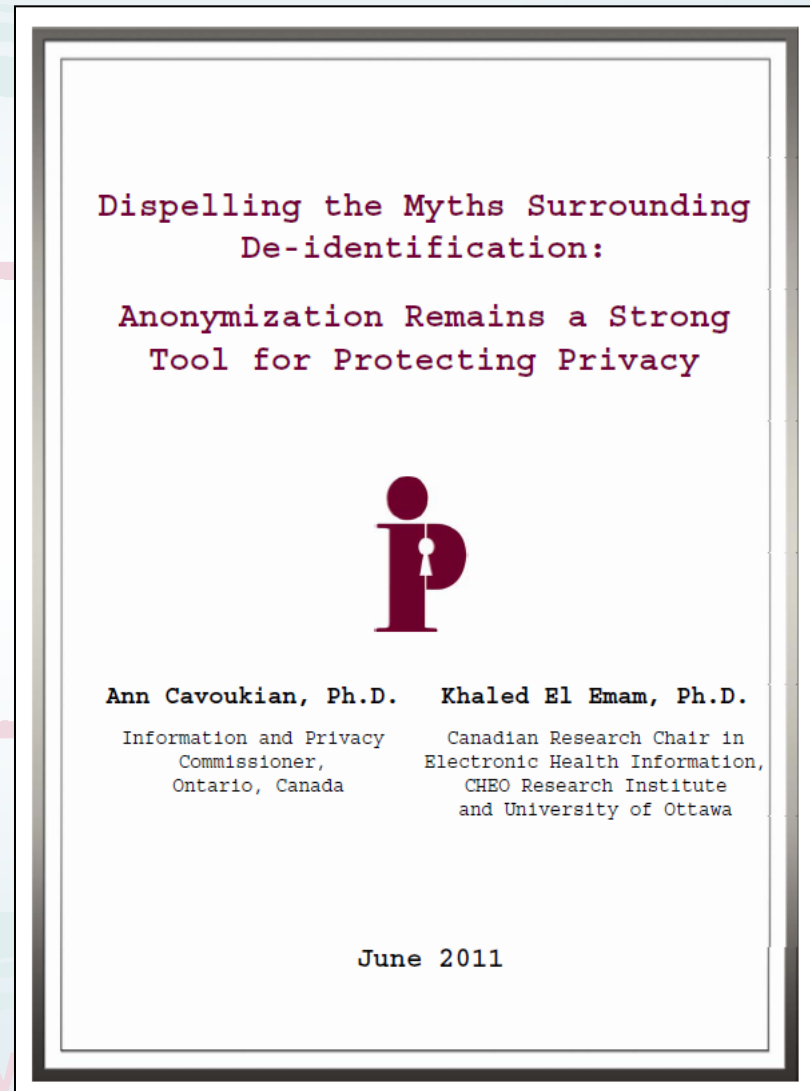
www.privacybydesign.ca

Data Minimization

- Data minimization is an essential safeguard in protecting personal health information, including for purposes of health research and analysis;
- Health care providers must not collect, use or disclose personal health information if other types of information (i.e. de-identified or anonymized) will serve the purpose;
- Health care providers must also not collect, use or disclose any more personal health information than is reasonably necessary to meet the intended purpose.

Dispelling the Myths about De-Identification...

- The claim that de-identification has no value in protecting privacy due to the ease of re-identification, is a **myth**;
- If proper de-identification techniques and re-identification risk management procedures are used, re-identification becomes a very difficult task;
- While there may be a residual risk of re-identification, in the vast majority of cases, de-identification will strongly protect the privacy of individuals when additional safeguards are in place.



Data De-Identification Tool

- Developed by Dr. Khaled El Emam, Canada Research Chair at the Electronic Health Information Research Institute; and a leading investigator at the Children's Hospital of Eastern Ont. Research Institute;
- De-identification tool that minimizes the risk of re-identification based on:
 - The low probability of re-identification;
 - Whether mitigation controls are in place;
 - Motives and capacity of the recipient;
 - The extent a breach invades privacy;
- Simultaneously maximizes privacy and data quality while minimizing distortion to the original database.



A Positive-Sum Paradigm in Action in the Health Sector

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner
Ontario, Canada

and

Khaled El Emam, Ph.D.

Canadian Research Chair in Electronic Health Information
CHEO Research Institute and University of Ottawa

A Zero-Sum versus Positive-Sum Paradigm

Individual rights are frequently pitted against societal rights or the public interest. When individual and societal rights collide, there is often an attempt to balance one against the other. The zero-sum paradigm dictates that the two goals (in this case, individual versus societal rights) are mutually exclusive and that each of the goals can only be attained at the expense of the other goal – the two goals can never be attained simultaneously.

Privacy is often viewed as an individual right that must be sacrificed in order to attain other socially desirable, but competing goals. For example, the right to privacy is often traded off to achieve national security goals. In the health sector, patient privacy may be sacrificed in the interests of health research and quality improvement. Over the years, the traditional zero-sum approach to managing competing goals has meant that privacy rights have been allowed to gradually deteriorate in favour of achieving other more urgent goals, such as minimizing a terrorist threat.

The Information and Privacy Commissioner of Ontario (IPC) is committed to bringing about a paradigm shift, by demonstrating how information technology, introduced to serve one function, can be designed and implemented in a manner such that privacy is maintained or enhanced, without derogating from the functionality of the technology. By building privacy into the design and implementation of information technology, the goal of protecting the individual's right to privacy and the original goal of the information technology can be attained simultaneously. This process, referred to as "Privacy by Design," shifts the traditional zero-sum paradigm to a positive-sum paradigm, in which both goals are maximized to the greatest extent possible.

Evidence that the Tool Works

- Dr. El Emam was approached to create a longitudinal public use dataset using his de-identification tool for the purposes of a global data mining competition – the Heritage Health Prize;
- Participants in the Heritage Health Prize competition were asked to predict, using de-identified claims data, the number of days patients would be hospitalized in a subsequent year;
- Before releasing the dataset created using Dr. El Emam's tool, the de-identified dataset was subjected to a strong re-identification attack by a highly skilled expert;
- The expert concluded the dataset could **not** be re-identified – Dr. El Emam's de-identification tool was highly successful!

Evidence that Re-Identification is Extremely Difficult

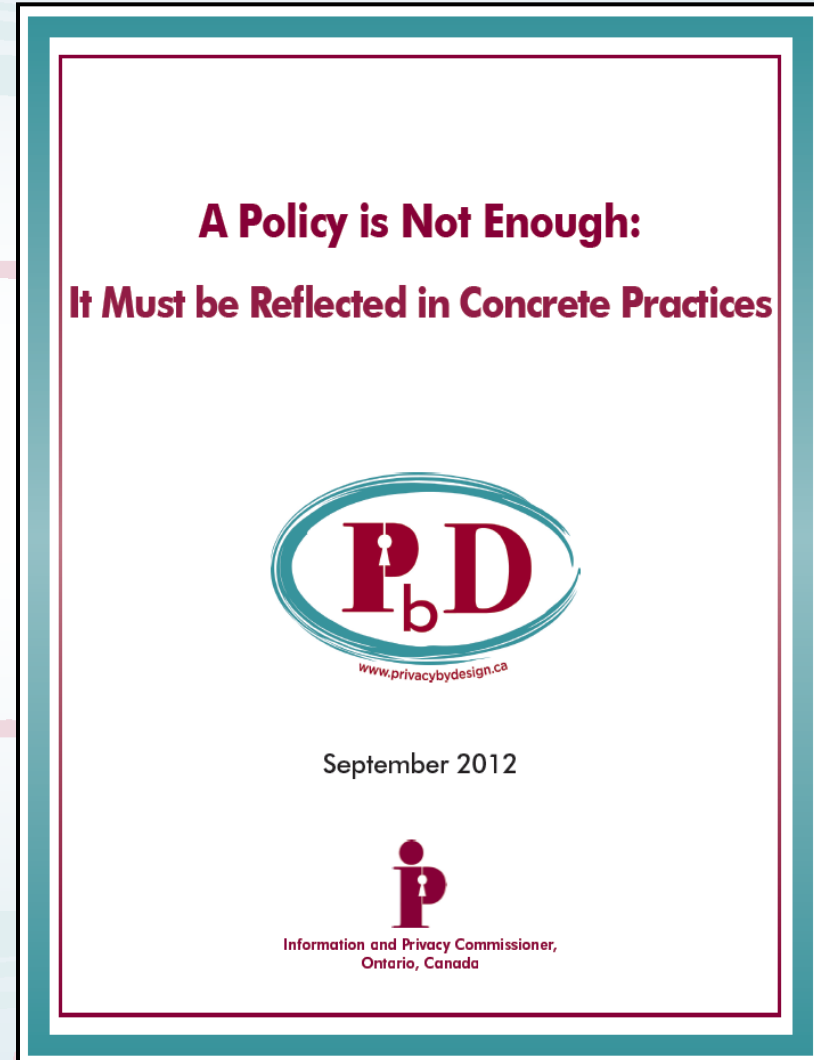
- A literature search by Dr. El Emam et al. identified 14 published accounts of re-identification attacks on de-identified data;
- A review of these attacks revealed that one quarter of all records and roughly one-third of health records were re-identified;
- **However, Dr. El Emam found that only 2 out of the 14 attacks were made on records that had been properly de-identified using existing standards;**
- Further, only 1 of the 2 attacks had been made on health data, resulting in a **very low re-identification** rate of **0.013%**.

Protocol for Data Linkages Without the Disclosure of any Identifying Information

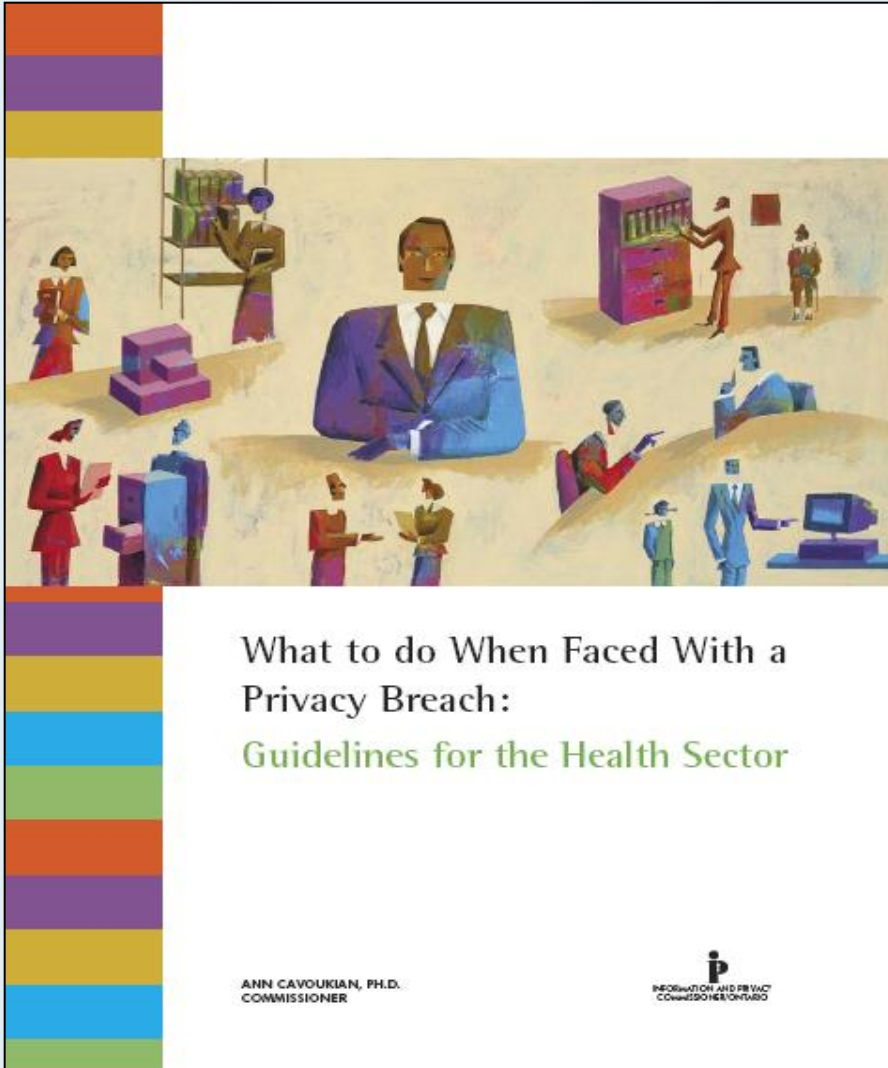
- Dr. El Emam has also developed a protocol for securely linking databases **without** sharing any identifying information;
- The protocol is described in an article with Dr. Craig Earle entitled *Secure Probabilistic De-Duplication of Databases*;
- The protocol uses an encryption system to identify and locate records relating to an individual that may exist in multiple datasets;
- It involves encrypting personal identifiers in each dataset and comparing the encrypted identifiers using mathematical operations, resulting in a complete list of matched records, without revealing **any** personal identifiers: All computations are performed on encrypted values;
- The protocol promotes compliance with existing prohibitions on the disclosure of identifying information in *PHIPA* by allowing for linkages to take place without the disclosure of any identifying information – a win/win, positive-sum solution.

A Policy is Not Enough: It Must be Reflected in Concrete Actions

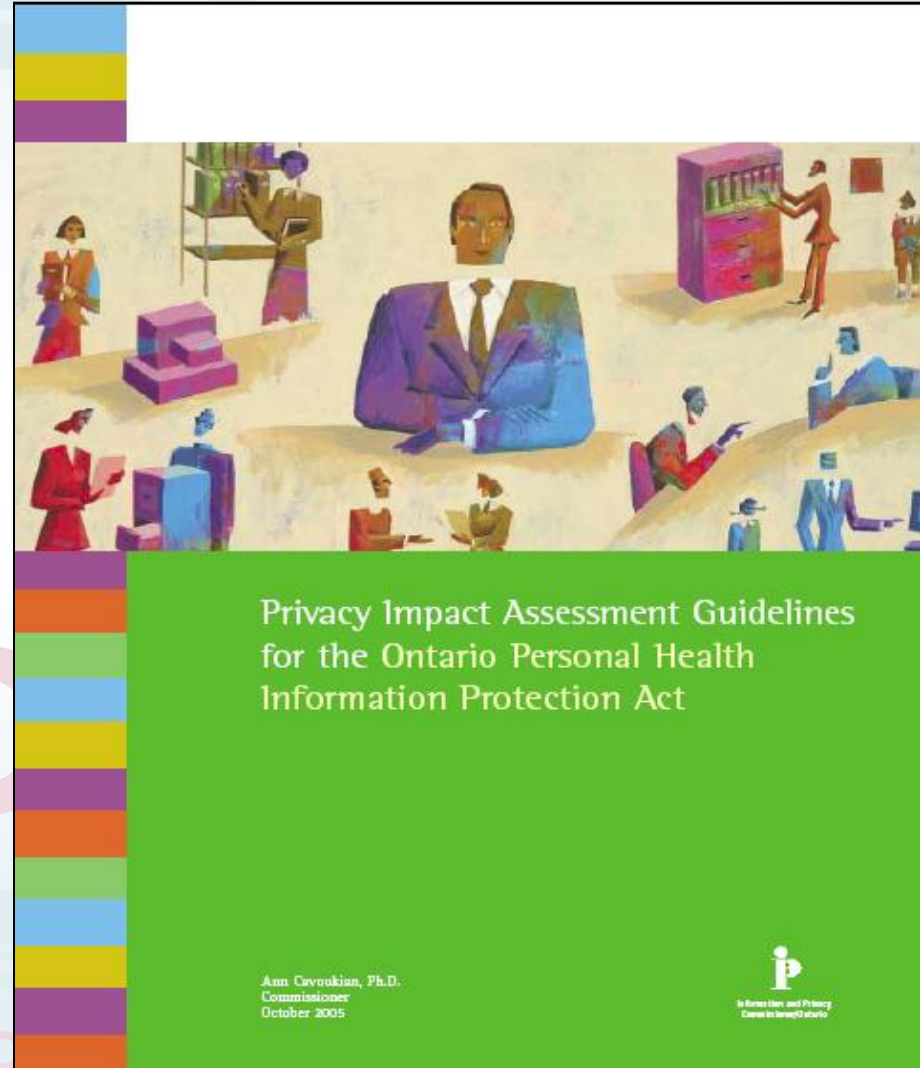
- Implement a privacy policy that reflects your privacy needs and risks;
- Link each requirement in the privacy policy to a concrete, actionable item;
- Demonstrate how each item will be implemented;
- Conduct privacy education and awareness training;
- Designate a central “go to” person for privacy-related queries;
- Verify compliance with privacy policies, procedures and processes;
- Prepare for a possible breach.



Implement a Privacy Breach Protocol ... Conduct a Privacy Impact Assessment



<http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=433>



<http://www.ipc.on.ca/English/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=574>

Stop. Think. Protect.



**... Protect Personal Health Information
on Mobile and Portable Devices**

Deter and Prevent Unauthorized Access

- Immediately terminate access to records pending an investigation into the issue of unauthorized access;
- Implement appropriate access controls;
- Consider the use of “VIP flags;”
- **Log and audit access to records;**
- Implement a policy of “zero tolerance;”
- Impose appropriate discipline for unauthorized access;
- Provide ongoing training using multiple means of raising awareness on appropriate access such as:
 - Confidentiality agreements;
 - Reminder notices displayed upon log-in to electronic records.

Conclusions

- Make privacy a priority – ensure that privacy is embedded into the delivery of health care services;
- It is far easier and more cost-effective to build in privacy up-front, rather than after-the-fact;
- Privacy risks may best be managed by proactively embedding the principles of *Privacy by Design*;
- Beware of unintended consequences;
- Get smart – lead with *Privacy – by Design*, not privacy by chance or, worse, privacy by Disaster!



PRIVACY
by
DISASTER

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 *Privacy by Design*,
please visit: www.privacybydesign.ca**