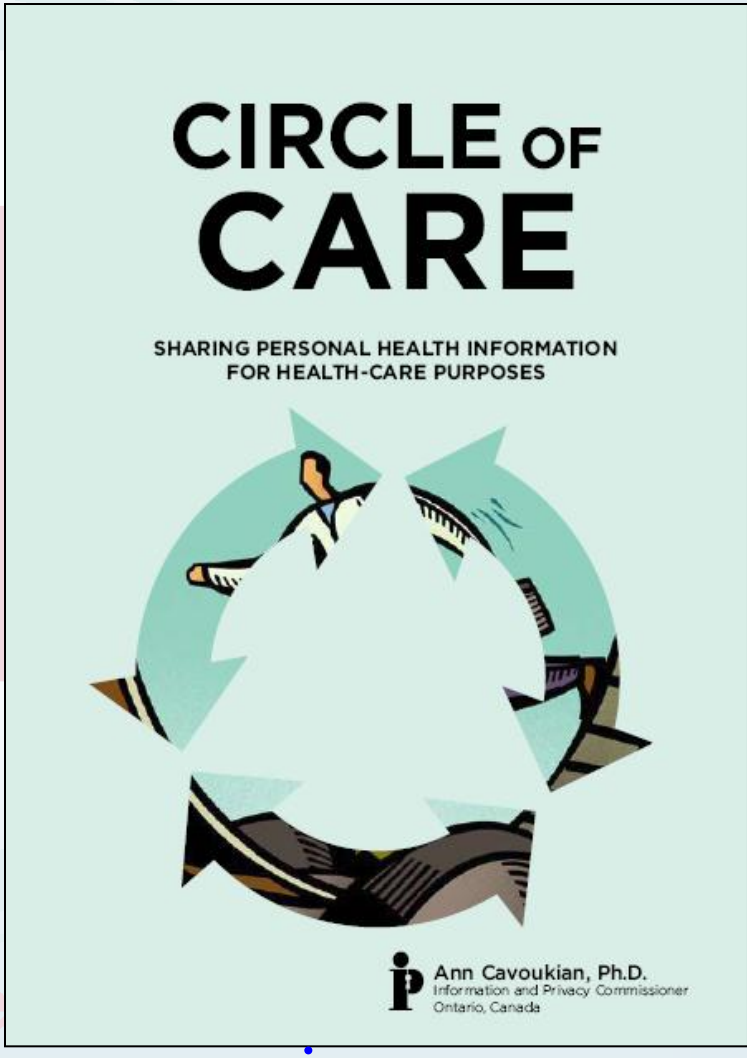
De-Identify Before Using Electronic Health Records for Secondary Purposes

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

Connecting GTA Executive Forum
April 11, 2013

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

- In 2009, we produced a guide to clarify the circumstances in which health information custodians may collect, use or disclose personal health information within the Circle of Care;
- Members of the working group included:
  - College of Physicians and Surgeons of Ontario
  - Ontario Long Term Care Association
  - Ontario Hospital Association
  - Ontario Medical Association
  - Ontario Ministry of Health and Long Term Care
  - Ontario Assoc. of Community Care Access Centres
  - Ontario Assoc. of Non-Profit Services for Seniors
  - Information and Privacy Commissioner of Ontario



www.ipc.on.ca

Circle of Care

- A health information custodian is permitted to imply **consent**, to collect, use or disclose personal health information for health care purposes, unless the individual states otherwise;
- This is commonly referred to as the "circle of care;"
- Outside this trusted circle of care, or for purposes other than the provision of health care, such as for secondary uses and disclosures, express consent must be obtained unless the collection, use or disclosure is permitted without consent.

Secondary Uses and Disclosures

- The *Personal Health Information Protection Act* ("*PHIPA*") came into effect on November 1, 2004;
- *PHIPA* recognizes the value of health research, quality improvement and analysis;
- *PHIPA* permits the use and disclosure of personal health information collected during the course of providing health care, for secondary purposes in appropriate circumstances;
- *PHIPA* attempts to ensure that these other purposes are achieved in a manner that minimizes the impact on privacy.

Research Purposes

- Health information custodians are permitted to collect, use and disclose personal health information for research purposes – the default is that consent be obtained;
- In exceptional circumstances, where obtaining consent is impractical, *PHIPA* permits the collection, use and disclosure of personal health information without consent;
- *PHIPA* ensures that appropriate safeguards are in place in those exceptional circumstances where personal health information is collected, used or disclosed without consent.

Quality Improvement

- Health information custodians are permitted to use personal health information for the purpose of:
  - Risk and error management;
  - Activities to improve or maintain the quality of care and related programs or services provided by the health information custodian.
- They are also permitted to disclose personal health information to other health information custodians if:
  - The individual to whom the information relates is or has received health care from both health information custodians; and
  - The disclosure is for improving or maintaining the quality of care provided to the individual or others who are provided similar care.

Analysis

- Health information custodians are permitted to use personal health information to plan, evaluate, monitor or allocate resources to programs or services they provide or fund;
- They are also permitted to disclose personal health information to:
  - A **prescribed person** who compiles or maintains a registry to facilitate or improve the provision of health care;
  - A **prescribed entity** for analysis or compiling statistical information with respect to the planning, managing, evaluating, monitoring or allocating resources to all or part of the health system; or
  - Public health agencies for public health purposes.

How Electronic Health Records Facilitate Secondary Uses and Disclosures

- Personal health information is often held in non-standardized paper format by individual health care providers;
- Even when this information is digitized, it is often contained within local systems that are not interoperable;
- Electronic health records can facilitate more secure and privacy-protective secondary uses and disclosures by:
  - Eliminating the need to convert and transfer paper records;
  - **Facilitating de-identification and creating repositories of de-identified information;**
  - Automating the collection, extraction and organization of common data elements from various repositories;
  - Providing longitudinal data for use in research and analysis.


PbD
www.privacybydesign.ca

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***.

PbD

www.privacybydesign.ca

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)*:

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy by Design Considerations

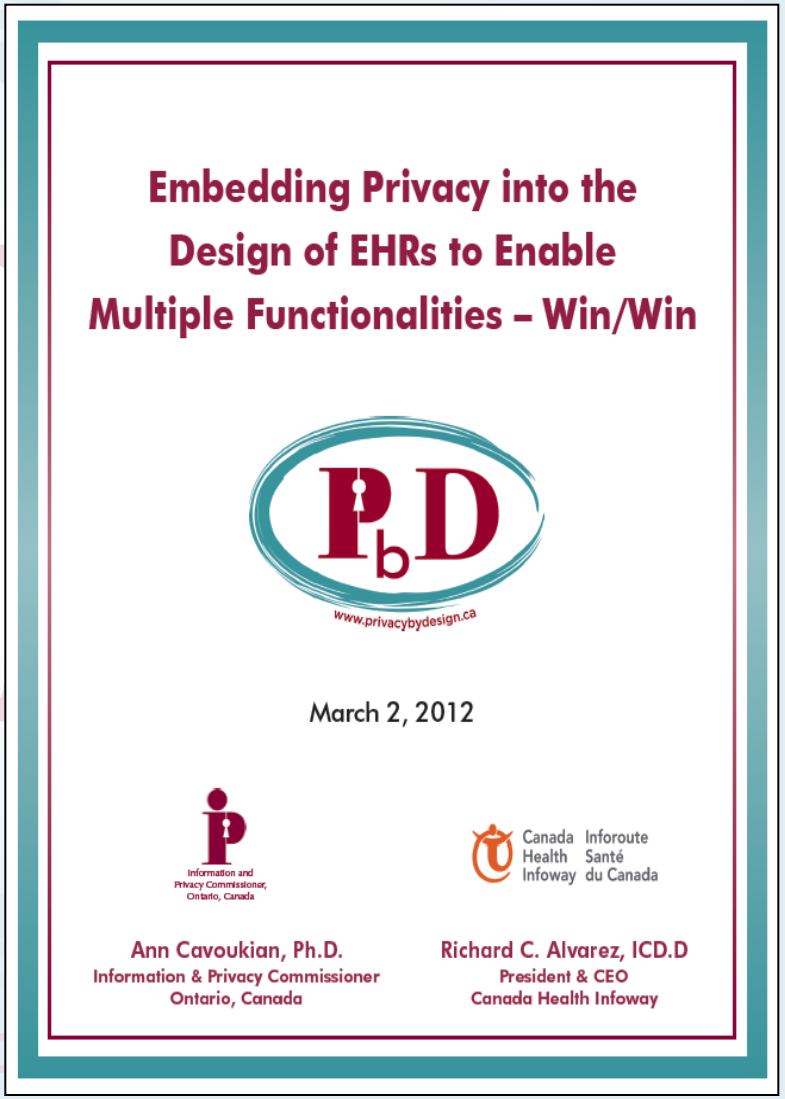
- Lead with *Privacy by Design* to enable *both* secondary uses and disclosures, **and** privacy;
- Be transparent about uses and disclosures for research, analysis and quality improvement purposes;
- **Ensure that de-identified information is used and disclosed as the default for such purposes – not identifying information;**
- Build de-identification tools directly into the processes and systems used for electronic health records;
- Use strong de-identification protocols and tools, (such as Dr. Khaled El Emam's de-identification tool), as well as re-identification risk measurement techniques.

Privacy by Design Considerations (Cont'd)

- Establish a framework governing how and by whom decisions about secondary uses and disclosures will be made;
- Amend existing legislation to provide such a framework;
- Ensure strong privacy oversight for secondary uses and disclosures;
- Embed privacy and security safeguards into the design and architecture of electronic health record systems.

Embedding Privacy Into Secondary Uses and Disclosures Involving Electronic Health Records

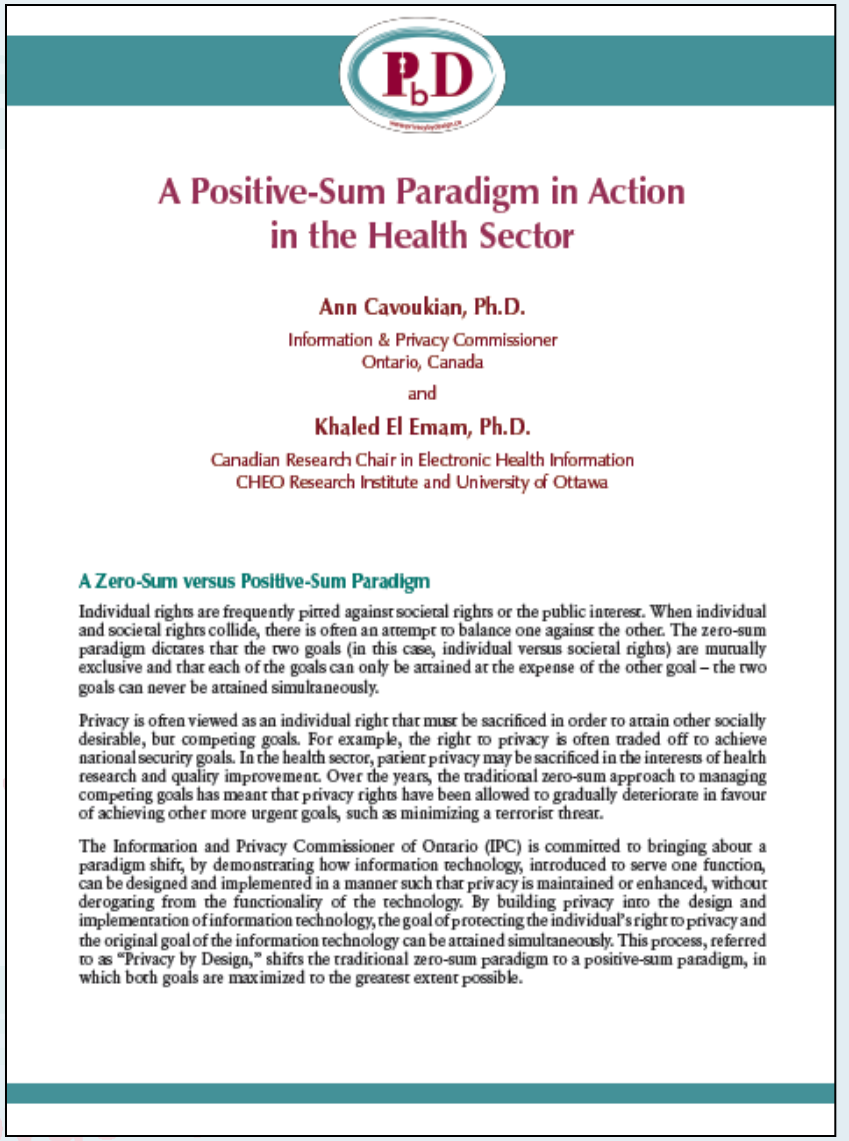
- My office published a white paper with Richard Alvarez, President and CEO of Canada Health Infoway;
- Electronic health records may be leveraged for socially beneficial purposes such as research, while maintaining strong privacy;
- De-identification must be the default if health information is to be used or disclosed for secondary purposes;
- Governance framework needed that includes legislation, policies and procedures; oversight; privacy-protective architecture; protocols for de-identification; data privacy and security training; and data breach protocols.



www.ipc.on.ca/images/Resources/2012-03-02-PbD-***EHR***.pdf

Data De-Identification Tool

- Developed by Dr. Khaled El Emam, Canada Research Chair in Electronic Health Information;
- 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, win/win solution.



PbD

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.

www.ipc.on.ca/images/Resources/positive-sum-khalid.pdf

Data Minimization for Record Linkages – Homomorphic Encryption

- Dr. El Emam has also developed a protocol for securely linking databases without sharing any identifying information;
- The protocol uses an encryption system to identify and locate records relating to an individual existing in multiple datasets;
- This involves encrypting personal identifiers in each dataset and comparing only the encrypted identifiers, resulting in a list of matched records without revealing any personal identifiers;
- The protocol promotes compliance with *PHIPA* by allowing linkages of datasets without the disclosure of any identifying information.

Conclusions

- Electronic health records have the potential to facilitate secure and privacy-protective secondary uses and disclosures;
- Lead with *Privacy by Design* to deliver full functionality – offer secondary uses, disclosures ***and*** privacy;
- One of the most important privacy safeguards for secondary uses and disclosures is data minimization – de-identify health information **before** contemplating any secondary uses and disclosures;
- The default should always be strong de-identification of health information **prior to** its use and disclosure for secondary purposes.

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