



The Ontario Health Study's Assessment Centres: A Case Study for “*Privacy by Design*”

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner
Ontario, Canada

and

Pamela C. Spencer

Cancer Care Ontario
VP Corporate Services, General Counsel & Chief Privacy Officer

Overview of *Privacy by Design*

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.

Traditionally, privacy has been viewed as an individual right that may be sacrificed in order to attain other socially desirable, but competing goals. For example, the right to privacy may be 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. Recently, 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 or containing a potential flu pandemic. To slow this persistent erosion of privacy rights, a fundamental paradigm shift is needed.

Privacy by Design is a concept that was developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, back in the 90's. At the time, the volume of personal information collected was growing, as were the risks posed by increasingly sophisticated and interconnected technologies. The Commissioner recognized that the future of privacy could not be assured solely through compliance with regulatory frameworks and legislation. Rather, organizations would need to operate in an environment of default privacy protection – embedding it as their standard mode of operation.

Initially, privacy-enhancing technologies (PETs) were seen as the solution. Today, we understand that a more substantial approach is required – by applying PETs in a positive-sum, not a zero-sum, manner. 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 individual privacy is maintained or enhanced, without derogating from the functionality, performance or security of the technology. By building privacy right into the design and implementation of information technology at the front end, the goal of protecting the individual's right to privacy and the original goal of the information technology can be attained simultaneously – shifting the traditional zero-sum paradigm to a positive-sum paradigm.

The IPC has extended the concept of *Privacy by Design* to a “Trilogy” of contexts – information technology systems, accountable business practices or processes, and physical design. Essentially, the principles of *PbD* may be applied whenever personal information is collected, used or disclosed, but should be applied with special rigor in the context of sensitive information, such as personal health information. Generally, the strength of the privacy protections that are built in should be commensurate with the sensitivity of the information and the degree of risk associated with exposure of the personal information.

Principles of *Privacy by Design*

The objectives of *Privacy by Design* may be accomplished by applying the following principles:

1. **Proactive** not Reactive; **Preventative** not Remedial

The *PbD* approach is characterized by proactive rather than reactive measures. The goal is not to mitigate privacy risks after they materialize or to remedy privacy breaches once they have occurred, but rather to mitigate potential risks up front and to prevent breaches from occurring in the first place. In other words, *Privacy by Design* comes before the fact, not after. In order to build in privacy, the potentially invasive aspects of a system, process or environment must be identified in advance of development and implementation. One way to identify threats early on is by conducting a Privacy Impact Assessment (PIA) during the project's conceptual stages.

2. Privacy as the **Default**

The goal is to deliver the maximum degree of privacy by ensuring that personal information is automatically protected in any given system, process or physical environment. Even if individuals choose to do nothing, their privacy should still remain intact. No action should be required on the part of the individual to protect their privacy – it should be built into the system, by default.

3. Privacy **Embedded** into Design

Privacy by Design requires that privacy is embedded into the design and architecture of systems, processes and physical environments. The goal is not to provide a retrofit or an add-on to address privacy issues that arise after the fact, but rather to incorporate privacy up front, as an essential component of the core functionality being delivered. As a result, privacy becomes integral to the system, process or physical environment, without diminishing its primary functionality.

4. **Full** Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner. This is in contrast to the old-fashioned, zero-sum approach, which forces unnecessary trade-offs among what may be perceived to be competing or incompatible goals. *PbD* dismisses false dichotomies, such as privacy versus security, by underscoring the obvious – that it is both essential and possible to have both.

5. End-to-End Lifecycle Protection

Privacy, having been embedded into the system, process or physical environment prior to the first element of personal information being collected, extends throughout the entire lifecycle of that information from collection through to disposal. Thus, *PbD* ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that the technology, process or physical environment functions according to the stated promises and objectives, particularly with respect to privacy. Fulfillment of these promises should be subject to independent verification. All aspects of the technology, process or physical environment should remain visible and transparent, to both users and providers alike. Individuals should never be expected to simply trust the system, process or physical environment – they must also be able to verify that it is worthy of their trust. Thus, *PbD* incorporates the adage – trust but verify!

7. Respect for User Privacy

Above all, *Privacy by Design* requires designers of systems, processes and physical environments to keep the interests of the individual uppermost by offering such features as strong privacy defaults, appropriate notice, and user-friendly privacy options. Keep it user-centric.

The Project: The Ontario Health Study

The Ontario Health Study (OHS) is a long-term, population-based, cohort study that will enable further comprehensive studies of cancer, vascular diseases, and other chronic diseases. The purpose of the study is to determine the causes of chronic diseases by looking at factors such as residence, employment, diet, exercise, and smoking habits. The OHS team aims to recruit approximately 150,000 Ontarians between the ages of 35 and 69 years, who live in diverse communities and represent the ethno-cultural diversity of the province, to participate in the study. Participants will provide their consent to the OHS team to collect information about their health (e.g. weight and blood pressure), family medical histories, work, community, and living environment and to use and disclose this personal health information for the purposes of the study. Participants will also provide biospecimens, such as blood and urine samples. The OHS will follow participants over the next 20 years, contacting them about once a year for additional information.

The OHS team will make de-identified information available to researchers, who have received Research Ethics Board (REB) approval, for research studies in the areas of cancers, vascular diseases, and other chronic diseases. Should researchers wish to collect additional information for their research studies, the OHS team will contact participants first to advise them of the researcher's request. If the participant agrees to participate in the researcher's study, the OHS team will collect the additional information on the researcher's behalf.

Participants may withdraw from the OHS at any time, in which case, the participant will no longer be contacted. However, the OHS team will continue to use information and biospecimens already provided for research purposes. Participants are informed of this in the study's Consent Form, which they must review and sign prior to joining the study.

The OHS Pilot Phase

The OHS, part of a national cohort initiative, is a partnership project by the Ontario Institute for Cancer Research, the Canadian Partnership Against Cancer, and Cancer Care Ontario. Cancer Care Ontario is responsible for the operation and management of the OHS. The Canadian Cancer Society (Ontario Division) and the Ontario Agency for Health Promotion and Protection support the objectives of the study.

The first phase of the OHS was the implementation of a Pilot study which took place between March and September 2009, and involved the recruitment of 1500 participants. The OHS used the information collected during the Pilot phase to assess the effectiveness of the baseline questionnaire, the recruitment strategy, and logistics of data collection, acceptability of data and biospecimen collection methods, functionality and security of IT protocols.

The OHS team received approval from the University of Toronto REB for its Pilot phase.

The Approach: Cancer Care Ontario's Privacy Leadership Role in the Ontario Health Study

Like many research studies, the OHS relies on volunteer participation. In order to encourage this participation and maintain participant trust throughout the term of the study, Cancer Care Ontario recognized the importance of *Privacy by Design* and ensured that they built privacy “best practices” into the study’s design. The OHS planning team identified privacy as one of the key work streams in building the Pilot study, and Cancer Care Ontario’s Chief Privacy Officer (CPO) assumed responsibility for the privacy work stream.

As a first step in the planning phase, the CPO appointed a Privacy Lead for the OHS. The OHS Privacy Lead developed privacy “best practices” that served to guide the activities of the study team, drafted privacy communications materials which provided participants full visibility of the end-to-end lifecycle protection of their personal health information, trained the study team on the privacy practices it must employ, worked with the study team to mitigate potential privacy risks, and advised the study team on all aspects of the pilot development and launch. In particular, the OHS Privacy Lead established the physical privacy measures that must be in place at the Assessment Centres to ensure the protection of participant privacy. These measures are outlined in a document referred to as a *Physical Review of Assessment Centres Best Practice*, included as part of a *Manual of Best Practices* that is used to provide guidance to OHS team members including third party contractors.

The Challenge: Design of the Assessment Centres

For the Pilot, the OHS established three assessment centres, one each in Mississauga, Owen Sound and Sudbury, representing urban, rural and northern Ontario communities. The Assessment Centres are the main point of contact for participants and the main information collection point for the Study. Eligible participants attend a 2-3 hour visit at their local Assessment Centre, where they provide their information and biospecimens for the purposes of the study. Visits to the Assessment Centre are scheduled via a Call Centre established by the OHS. Call centre staff have been trained on privacy best practices.

Demonstrating the broad scope of the seven foundational principles of *PbD*, the Assessment Centres and their processes reflect the fact that patient confidentiality has been built in. Each Assessment Centre contains five distinct stations at which participants provide their health information and biosamples to trained staff. First, a participant checks in at reception, where the receptionist provides the participant with a bar-coded badge to wear which is linked to a unique Participant ID. This ID is used to identify

the participant throughout the assessment. The barcode is also included on pre-printed labels for blood and urine collection tubes. Second, the participant reads and signs the consent form to participate in the study. Only if the participant consents does he or she complete the online self-assessment questionnaire, which includes questions about health, diet, exercise routine, and home and work environment. Third, the participant meets with a registered nurse to answer questions about his or her current medications and personal and family medical history and to record blood pressure and resting heart rate. Fourth, physical measures are taken, such as standing and sitting height, waist and hip circumference, grip strength, bone fragility, and spirometry. Finally, the participant provides a urine and blood sample. Anticipating areas where patient confidentiality might potentially be compromised, this approach exemplifies a preventative posture with respect to protecting personal health information.

At the end of the visit, the nurse manager meets with the participant, provides the participant with a copy of his/her consent form and a report outlining physical measures results, and answers any questions the participant may have. Where the nurse determines that a participant's physical measures are unusually high or out of range, the participant is advised to visit his or her family physician.

The Solution: A Blueprint for Participants' Physical Privacy

Given the unique purpose for, and temporary nature of, the Assessment Centres, the OHS team faces the challenge of finding a location that accommodates the required number of stations, and allows for participants' physical privacy. The physical privacy afforded by these sites is a top priority because in order for the study to be successful, participants must feel comfortable providing intimate details of their health history at the Assessment Centre. To this end, the OHS builds physical privacy into the Assessment Centre design by addressing it as part of site design, equipment procurement, and training, and reviewing the implementation of physical privacy measures before the Assessment Centre can be opened. Each of these steps is discussed in turn below.

The Design

The Privacy Lead works with the OHS team to develop a model floor plan for the Assessment Centre that takes into account the physical privacy measures. For example, the questionnaire stations, where participants use touch screen monitors to enter their personal health information into the study database, are designed with dividing walls. This prevents participants from viewing the information on the screens of participants sitting next to them.

Where the OHS Privacy Lead cannot visit the Assessment Centre in person due to distance, the Lead relies on digital pictures or webcam videos of the site to supplement the information contained in the site floor plans and with the Privacy checklist described below.

The Equipment

The Privacy Lead collaborates with the OHS team to procure the information technology and office equipment required for the Assessment Centre. For example, all computers used at the Assessment Centre are encrypted and computer monitors are located out of view of other participants. Further, the computer monitors in the interview rooms are set up to easily turn toward the participant. This enables the participant to view his or her personal health information as the nurse is entering it into the study database.

The Assessment Centre staff scan the participant's bar-coded badge with hand-held scanners at each station to identify the participant by his or her unique numbered ID, not their name. This enables the study to de-identify participant information at each subsequent station before it is entered into the study database. Moreover, this is an important data quality measure to ensure the information entered into the database is accurately associated with the right participant.

Data is never stored on local computer hard drives. All the personal health information collected at the Assessment Centre is stored on a central server, which is housed in an enclosed, locked cage in a room separate from participants. On a nightly basis, this information is transferred to the secure data centre at Cancer Care Ontario.

Training

All Assessment Centre staff have been trained before beginning work with the study. This training serves to, among other things, educate them on the privacy practices they must employ at each Assessment Centre station. For example, the receptionist is trained to escort participants to the questionnaire stations and to stagger participants' placement. The receptionist is also trained to provide a pad of paper to participants should they prefer to write personal information, instead of saying it aloud, upon registration. All Assessment Centre staff are trained to answer common privacy questions (e.g. "who has access to my information?"). Lastly, a Privacy Information factsheet is made available to participants at the Assessment Centre and on the study's website, outlining the information the study will collect; how it will use, disclose and safeguard the information and biospecimen samples; and the participants' right to withdraw from ongoing contribution to the study.

The Review

A model *Physical Privacy Review Checklist* has been developed to permit the Privacy Lead to assess the Assessment Centre before the site is opened to participants. This Checklist includes the equipment that must be in place at each Assessment Centre station and instructions regarding how the equipment must be set up. Where the OHS Privacy Lead cannot attend the Assessment Centre in person, this function is delegated to a senior on-site OHS team member.

Given the world-class research that will result from the Ontario Health Study and the importance of having complete and high quality data available to improve the prevention of cancer, vascular diseases, and other chronic diseases, Cancer Care Ontario recognizes that privacy must be an essential part of the participant intake process. The positive-sum nature of *Privacy by Design* has ensured that the OHS team could build privacy measures into the design of the Assessment Centres as well as their processes and satisfy the overall objectives of the study.

To participate in the Ontario Health Study or to learn more, visit: www.ontariohealthstudy.ca.

The Ontario Health Study is conducted with the support of the Ontario Institute for Cancer Research through funding provided by the Province of Ontario, the Canadian Partnership Against Cancer and Health Canada. The views expressed herein do not necessarily represent the views of Health Canada or the Public Health Agency of Canada.



About the Authors

Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protection. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in a number of international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening trust and confidence in emerging technological applications. Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada and is a member of the Future of Privacy Advisory Board. Reappointed as Commissioner for an unprecedented third term, Dr. Cavoukian intends to grow *Privacy by Design* and hopes to make it go "viral."

Pamela C. Spencer, Vice-President, Corporate Services, General Counsel and Chief Privacy Officer, Cancer Care Ontario, Certified Health Law Specialist, Law Society of Upper Canada

Ms. Spencer graduated from Osgoode Hall Law School in 1987 and was admitted to the Ontario Bar in 1989. In addition to her law degree, Ms. Spencer holds a Bachelor in Social Sciences from the University of Ottawa, and a Masters in Health Science in Health Administration/Collaborative Program in Bioethics from the University of Toronto, Faculty of Medicine, Department of Health Policy, Management and Evaluation.

Prior to joining Cancer Care Ontario in 2003, Ms. Spencer practiced corporate commercial law, specializing in the health sector, at Fraser Milner Casgrain LLP where she was Chair of the Toronto Health Law Group and co-Chair of the Toronto Privacy Law Group. Ms. Spencer is responsible for a diverse portfolio at Cancer Care Ontario including Legal, Procurement, Facilities, Privacy & Access and the Board Secretariat. Ms. Spencer is also co-Executive Sponsor of the Ontario Health Study, a provincial population-based cohort study which has as its goal the enrollment of 150,000 health Ontario participants by 2012 for baseline data collection.

Ms. Spencer is a member of the Canadian Bar Association and the Medico-Legal Society of Toronto. She is former Chair of the Ontario Bar Association, Health Law Executive and former Chair of the Law Society of Upper Canada, Health Law Specialist Certification Committee.

Ms. Spencer has written and lectured widely on many aspects of health law and health privacy.



Published: April 2010

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario • M4W 1A8 • Canada

Telephone: 416-326-3333 • 1-800-387-0073

Facsimile: 416-325-9195

TTY (Teletypewriter): 416-325-7539

E-mail: info@ipc.on.ca

Web site: www.ipc.on.ca