OCRI

Electronic Health Information & Privacy

2006
Electronic Health Information & Privacy Conference

November 13, 2006 – Ottawa, Canada

Gold Sponsors

CHEO Research Institute / Institut de recherche

Microsoft®

Silver Sponsor

Camouflage™ DATA MASKING SOFTWARE

Media Sponsor

Ottawa Citizen

Supporters

Canadian Healthcare Technology

COACH

ITAC Information Technology Association of Canada

Program

-- REGISTRATION (8:00-8:30) --

-- OPENING STATEMENTS, Congress Hall A (8:30-8:45) --

Plenary

Congress Hall A (8:45-9:45)

Health Chips? Using Implantable RFID to link Patients to Health Records
Ian Kerr

-- BREAK (9:45-10:15) --

Track 1 Congress Hall A	Track 2 Capital Hall 1B
Session 1 (10:15-12:00)	Session 1 (10:15-12:00)
Overview of Health Policy as it Pertains to Electronic Personal Health Information Ross Hodgins	Privacy Considerations During the Implementation of Electronic Health Records Glen Geiger
Legal Challenges Surrounding Electronic Health Record Systems Patricia Kosseim	Information Privacy and Security Implementation for Healthcare: Policy, Process and Progress Jeff Curtis
Managing Security Incidents involving personal information: What to do when the unthinkable occurs Michael Power	Inter-jurisdictional sharing of health information among Federal, Provincial and Territorial Governments for Public Health Management Jeannine Parent

-- LUNCH (12:00-13:00) --

Session 2 (13:00-14:45)	Session 2 (13:00-14:45)
For Better, Not Worse: Data Protection and Health Research Val Steeves	What do Canadians think about electronic health information and privacy? A systematic review of public opinion surveys and trends, 1999-2006. Mary Lysyk
A qualitative picture of identity theft and its implications for e-health Dr Gordon Atherley	“Sorry, You Can’t Have That Information” Stakeholder Awareness, Perceptions and Concerns Regarding the Disclosure and Use of Personal
National Privacy and Security Guidelines: A Canadian Experience in Jurisdiction-Wide Use	

Elaine Sawatsky	Health Information Angela Power and Dr. Daryl Pullman,
	Living the nightmare: notifying affected persons after a privacy breach Catherine Tully
-- BREAK (14:45-15:15) --	
Session 3 (15:15-17:00)	Session 3 (15:15-17:00)
The re-identification of anonymized records in Ontario Khaled El Emam (PhD)	Privacy Enhancing Technologies: A Microsoft Perspective Steve Heck
Statistical Disclosure Control Techniques and Issues Jean-Louis Tambay	Technology Aids Privacy Compliance in Healthcare Michael Gurski
Consumer Information as Commodity: The Databrokerage Industry & its Implications for Health Privacy Philippa Lawson	Applications of Data Masking Technology in Practice Paul Preston
- CLOSING STATEMENTS, Congress Hall A (17:00-17:30) -	

Table of Contents

Electronic Health Information and Privacy

Introduction

The importance of Information technology (IT) to the health care industry is rising as organizations attempt to find ways of reducing the costs of care, and improving patient safety. However, the ease of storage and exchange of large volumes of data electronically has raised many privacy questions among the public, patients, clinicians, Research Ethics Boards (REBs), hospital IT departments, and researchers.

Following last year's very successful Electronic Health Information and Privacy Conference, we are expanding the event and focusing on more specific topics. This year's topics are critical for framing the dialogue about the adoption of IT in health care, privacy, and security. The conference is covering contemporary issues that have gained prominence over the last twelve months, such as: the Canadian public's perception of the privacy of their electronic health information and how they think it should be used and disclosed; privacy legislation in Canada and its relationship to the electronic health record; the costs and value of notification; best practices for dealing with a breach; updates on practices for de-identifying health information; what are RFIDs and their risks, if any; definition and pervasiveness of identity theft in health care; and experiences and lessons learnt from the implementation of electronic health records.

Khaled El Emam
University of Ottawa

A qualitative picture of identity theft and its implications for e-health

Dr Gordon Atherley, Principal, Greyhead Associates

Abstract:
Identity theft, among the fastest growing crimes in North America, is making consumers increasingly wary of information technology systems that capture their personal data. Through the activities of organized crime and other factors, it is encroaching on Canadian healthcare. Governments can at this time reassure neither patients nor the physicians, pharmacists, nurses and the other healthcare professionals who provide patients with care that their identities are fully protected throughout the healthcare system. Enhancement of healthcare's prevention and protection, already requirements under Canada's health information and privacy laws, becomes urgent for the electronic health record and other e-health applications and for eligibility verification within the administrative domain. Together, these comprise a pressing responsibility for healthcare as well as governments.

Bio:
A physician retired from active practice, Atherley holds the British equivalent of the Canadian PhD and MD degrees, and LLD, Honoris Causa, from Canada's Simon Fraser University.

In academia, he held senior, tenured positions including Chair, at the UK Universities of Manchester, Salford, and Aston in the Faculties of medicine, physics, and engineering, respectively. In Canada he was Professor of Occupational Medicine at the University of Toronto. He is the author of an authoritative textbook and has 50 refereed publications in indexed journals.

Through Greyhead Associated, he provides research, analysis, and solution-development services to public-sector agencies, major hospitals, professional associations, and corporations on complex problems arising out of the use of information technology in healthcare.

His involvement in healthcare and research includes reviewer for the Canadian Medical Association Journal, adviser to PhD students, authoring for quasi-learned and general-interest publications, involvement in university research projects, lecturing, membership of advisory committees, involvement with professional associations, and life membership of the Canadian Medical Association and the Ontario Medical Association.

A qualitative picture of the role of identity in e-health risks

The case for rigorous, independent research

Dr Gordon Atherley
Greyhead Associates
atherley@sympatico.ca

Argument

1. Most sectors of application of IT to human affairs are subject to threats
2. Common to many threats is a person, organization or thing purporting to be somebody or something else
3. ID abuse and other sources of inaccuracy of identity data are thus risk factors in IT

Argument, continued

4. Because healthcare employs the same IT as other sectors, we cannot assume its immunity to identity-related threats
5. Whence the need for ***epidemiological study*** of health-related risks associated with identity-related threats in healthcare

Epidemiology to study risk

- Epidemiology's methods embrace *descriptive* and *inferential* statistics
- Prerequisite for both are ***accurate qualitative pictures*** of ID-related risks
- Piecing together the qualitative pictures requires empirical observations from documented occurrences, credible experiences, and plausible parallels

Greyhead Associates

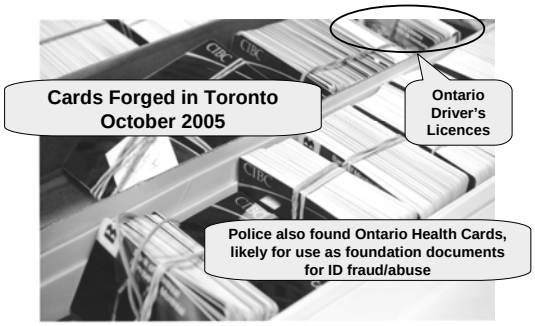
Example of a qualitative picture: fraud and ID abuse, Ontario, May 2006*

- Through **title fraud** a property was stolen from an 89-year-old man, Paul Reviczky
  - ⌦ The tenants renting the property used false names
  - ⌦ The tenants forged a power of attorney authorizing a fictitious grandson, Aaron Paul Reviczky, to sell the property
  - ⌦ The power of attorney was notarized to the effect that
    - the grandson is personally known to a lawyer
    - he produced a Driver's Licence as ID
- The bogus grandson's sale of the property to an innocent buyer is recognized as valid under Ontario law

*Sources: Toronto Star and Toronto Sun

Greyhead Associates

ID-related link with healthcare*



*Source: The Toronto Sun

Greyhead Associates

ID-related risk in healthcare

- Qualitative pictures from six contexts of ID-related risks, all highly sensitive socially, ethically and politically

Greyhead Associates

1. Tainted-blood catastrophe, 1980s

Krever Commission (1997) report on Canada's blood supply:

- alleged the Red Cross and the federal and provincial governments ignored warnings and acted irresponsibly in the testing of blood for HIV and Hepatitis C
- estimated that over 28,000 people contracted Hepatitis C from blood transfusions between 1986 and 1990
- concluded that some 85 percent of these infections could have been prevented had the Red Cross and governments acted appropriately

⌦ ID-related risks played an important part in the catastrophe

Greyhead Associates

1. Tainted-blood catastrophe, contd

Krever found that

- in 1986, reports were published that hemophiliacs using a medical product had been infected by HIV
- although the reports did not identify the product by name, they gave enough information to identify it
- Health Canada's Bureau of Biologics did not recognize the identity of the manufacturer from the reports, and did not seek additional information to do so. It therefore did not demand that the product be recalled or withdrawn

⌦ ID-related risk—Failure to accurately identify a medical product contributed to the catastrophe

Source: Krever Commission Report, Vol 3 p993

Greyhead Associates

1. Tainted-blood catastrophe, contd

Krever:

- "would also have expected that the Red Cross would carefully weigh its concerns about shortages of blood components and about potential discrimination against high-risk groups [Haitians, homosexual men] against the possibility that AIDS, a fatal disease, could infect the blood supply"

⌦ ID-related risk—Identification of groups as well as individuals created social and ethical challenges that increased risk to patients because of reluctance to fully use ID data

Source: Krever Commission Report, Vol 1 p293

Greyhead Associates

2. Risks of donor organ supply*

Shortages in organ supply are at crisis levels worldwide: thus organs come from many and possibly unknown sources

- Transplant teams must assure recipients that diseases are not transmitted from donors
- Donors are often cadavers, but now more and more are living persons
- Donor's medical and social history is the first and most important screen against donor-to-recipient transmission

⌦ ID-related risks (cf Krever)—How can it be known if a

- cadaver's medical record is corrupted by ID abuse or error?
- living donor's medical record is corrupted by ID abuse or error?

*Source: New Developments in Transplantation Medicine, Summer 2006

Greyhead Associates

3. Fraud by MDs, RPhs*

- Fraud by MDs and RPhs involves billing OHIP for services and drugs not actually delivered to individual patients
- Ontario MOHLTC doesn't attempt to detect and correct patient data corrupted by fraud

⌦ ID-related risk—The patient's ID has been abused, risking propagation of corrupt data through an interoperable eHR system

*Source: Ontario Provincial Police reports of charges laid

Greyhead Associates

4. Undocumented person/illegal immigrant*

- Undocumented persons by force of circumstances buy IDs on the street, using ***foundation documents***

⌦ ID-related risks—

- Key aspects of the ID abuser's medical history may be never be known
- The eHR may propagate a medically misleading picture of the ID abuser

*Sources: CBC documentary; police reports, 2006

Greyhead Associates

5. IVF / assisted reproduction*

- A biological parent uses a false ID
- Data entered in the parent's medical record is thus false
- False data including genetic information may pass from the parent's electronic health record to that of the unborn child

⌦ ID-related risks—

- Who will this child be genetically?
- What are the medical, legal and social consequences of propagating inherited data that is wrong?

*Source: Sabatini L, et al (2006) St Bartholomew's and The London NHS Trust

Greyhead Associates

6. Therapeutic abortion*

- Patient uses someone else's health card—and thus health record—to be eligible for the procedure
- Hospital concerns include risk of incompatible blood transfusion

⌦ ID-related risk— Relying on the interoperable eHR's false data on blood type preparatory to a blood transfusion

*Source: Society of Obstetricians and Gynaecologists of Canada

Greyhead Associates

Initial summary of QP's, 1

Harmful human factor	Use/abuse of ID	Medical risk
Fraud by health professional	Patient's ID abused	eHR propagates erroneous data
Fear of causing offence	Donors' IDs not properly identified	Blood transfusions contaminated
Failure to heed warning	ID not sought of risky product maker	Contaminated product not pulled
Trust in Cadaver's unreliable record	Cadaver's ID unverifiable	Contaminated organ transplanted

Greyhead Associates

Initial summary of QPs, 2

Harmful human factor	Use/abuse of ID	Medical risk
Trust in donor's unreliable record	ID unverifiable	Contaminated organ transplanted
Individual uses false identity	ID abuser is patient	eHR propagation of gaps or errors
Individual conceals true identity	ID abuser is biological parent	eHR propagation of false data on child
Individual conceals true identity with another's health card	ID *abuser* is patient ID *abused* may be another patient	Risk of incompatible transfusion, other medical error

Greyhead Associates

Case for rigorous, independent research

Research should proceed into the first-sight case that

- healthcare IT is not immune to threats experienced in other sectors
- some threats in healthcare risk of harm to the health of persons and not just invasions of privacy
- weaknesses in the processes by which ID is allocated and validated enable or facilitate some threats
- invalid ID aggregates erroneous data to health records
- interoperable eHRs propagate health records with erroneous data
- public concerns are growing about IT's abilities to protect citizens against harm facilitated or enabled by IT

Greyhead Associates

Coda

- To pursue the rigorous, independent research would be to attorn to a core ethical principle of healthcare—which holds that risk to patients must be researched, acknowledged and confronted

Greyhead Associates

Information Privacy and Security Implementation for Healthcare: Policy, Process and Progress

Jeff Curtis, Sunnybrook Health Sciences Centre

Abstract:
Since the Personal Health Information and Protection Act came into force in November 2004, hospitals and other healthcare providers have had enough time to establish their compliance with the law, but how effective has our collective implementation been in accomplishing the intent of the Act and its regulations? This talk will highlight some of key legal provisions that have informed our hospital's policy and process decisions over the past 2 years and will reflect on several of the areas where more work needs to be done to satisfy all of the privacy interests that claim a stake in this important information management component.

Bio:
Jeff Curtis is the Coordinator for Sunnybrook Health Sciences Centre Privacy Office in Toronto. Jeff also participates in Strategic Planning, Board Governance and Information Technology related planning activities at the hospital. Jeff has worked in the Information Technology sector for the past 16 years, and began his career 22 years ago as an economist with Consumers Gas (now Enbridge) in Toronto. Jeff has an undergraduate degree in Economics and an MBA from the University of Toronto.

"Responding to Hospital Information Privacy and Security Requirements"

Presented by
Jeff Curtis, Coordinator, Privacy Office
Sunnybrook Health Sciences Centre

November 13, 2006

Presentation Agenda

1. **Organizational Privacy Issues**
2. **Privacy Policy Development & Implementation**
   - **Lockbox Overview**
3. **Towards a Security Framework for Healthcare**

Organizational Privacy Issues

- Public perception of a legitimate privacy framework extends beyond established professional obligations and requires clear legal basis and application.
- Resolution of public benefit vs. individual harm tradeoffs – policy and procedures are increasingly required to establish rights and obligations and to resolve disputes.
- Increasing use of electronic records: era of transition to de-centralized information control and proliferation of data formats requires new standards, policy and procedures.
- Scale and scope of 'legitimate' information access is growing as service design and delivery becomes complex.
- Government recognized as having a role in facilitating access and ensuring patient rights – both federal and provincial authorities are in motion on this.

Organizational Privacy Issues

Privacy is a component of Information Security:

- More on a security framework approach later…
- A secure approach facilitates access to, accuracy of and confidentiality of personal health information
- A balanced approach across all three aspects is required to achieve acceptable results at reasonable cost.
- Hospitals already address security aspects in compliance with existing legal requirements, established health professional standards, and industry best practices:
  - Public Hospitals Act
  - Regulated Health Professionals Act
  - Hospital Accreditation Standards
  - Sunnybrook Medical Dentistry and Midwifery By-Laws
  - Recognition of Tri-Council Policy for Research Ethics
  - PIPEDA and PHIPA

Organizational Privacy Issues

- Traditional information privacy approaches can lack cohesion in a healthcare setting however, due to:
  - Need to consistently balance patient rights and hospital obligations during all collection, use and disclosure
  - Need to recognize multiple record handlers who may have or perceive varying obligations under other statutes or codes of practice
    - Some roles identified in PHIPA, but few are named entities;
    - Prevailing obligations under PHIPA remain subject to interpretation on a case-by-case basis – little regulation
  - Multiple, existing hospital policies, procedures and contracts that have embedded privacy obligations – our ongoing review through a "privacy lens" (legal or ethical) has revealed best practices but also areas that require alignment

Organizational Privacy Issues

Collection:

- Physically distributed across 2+ campuses among several thousand medical and admin staff; "agent" role can be difficult to enforce with independent care professionals
- Data capture is increasingly decentralized and multi-modal: includes centralized and clinic-based records; paper and electronic capture; paper, verbal, fax and email modes of transmission; direct and indirect capture from patient.
- Multiple copies of a 'record' or record components may be generated by different caregivers
- Collection (and use) of the 'same information' may be inconsistent between authors, procedures and applications
- Patient notice of collection purposes (required by PHIPA) has increased public scrutiny; need for policy and legal clarity with plain language explanations

Organizational Privacy Issues

Use:

- Role-based access (authorization + authentication) is difficult to implement without compromising patient care since "need-to-know" is largely prospective and dynamic (e.g. people change jobs; roles change throughout the day; not always clinically convenient to constantly log on/off...)
- Password-based authentication (single factor authentication) remains a cost effective but weak form of user identification:
  - Proliferation of passwords doesn't enhance security and may promote workarounds (e.g. password reuse and sharing)
  - Resulting audit capabilities can be limited since individuals can always claim no knowledge of their physical access.
- Direct care use is generally not the problem!: Managing patient expectations and use/disclosure beyond direct care (e.g. Fundraising and Research) becomes the focus for enhancing current policy and procedures

Organizational Privacy Issues

Disclosure:

- Established practices between custodians and 3rd parties may conflict with interpretation in law or policy.
  - Increased need for privacy reviews, impact assessments and review of standardized approaches
  - Disclosure contracting and legal review adds cost, time and complexity to service delivery partnerships
  - Not all providers are prepared for more formality
- Use of lockbox to protect information between providers require more patient dialogue, procedural changes for record keeping and consistent notification to users.
- Required notice of collection cannot list all possible disclosures (e.g. to registries)...a growing list with no obvious public expectations.

Presentation Agenda

1. **Organizational Privacy Issues**
2. **Privacy Policy Development & Implementation**
   - **Lockbox Overview**
3. **Towards a Security Framework for Healthcare**

Policy Statement

"It is Sunnybrook's Policy to ensure that all transactions involving the use of personally identifiable patient information respect the privacy rights of individuals.

Personal Health Information will be collected, used and stored in a confidential and secure manner, while being made available to authorized users for patient care, administration, education, research and other third party authorized purposes."

Privacy Policy at Sunnybrook

Sunnybrook collects and uses personal health information for the purposes of:

- Providing health care or assisting in providing health care to the individual;
- Planning or delivering patient care programs or services funded by Sunnybrook;
- Evaluating, monitoring and allocating resources to these programs and services;
- Activities to improve quality of care or quality of any related program or service;
- Processing, monitoring, verifying or reimbursing claims for payment under any Act;
- Research, as approved by a Research Ethics Board;
- Teaching and education;
- As otherwise consented by the individual

Privacy Policy at Sunnybrook

Privacy Policy Application:

- Policy development acts as a "privacy lens": integrates existing hospital information handling policies and procedures with privacy legislation and best practice
- Establishes ten principles of accountability for collection, use and disclosure
- The basis for day-to-day Privacy Office operations:
  - Consistent policy response and legal interpretation
  - Establishes CPO, agent and partner accountability frameworks
  - Ongoing Privacy Reviews and Privacy Impact Assessments
  - Use in Auditing and Incident Reporting

Key Sunnybrook Policy Messages

- Personal Health Information belongs to the patient.
- Sunnybrook is the custodian of patient information and is accountable for its collection, use, disclosure and retention.
- Access to patient information is a privilege.
- It is a shared responsibility to protect the privacy of personal information at Sunnybrook – staff and patients should be aware of our policies and procedures.

Privacy Implementation Challenges

Centralizing Patient Opt outs:

- Fundraising: Foundation vs. departmental approaches?
- Research: when does 'impractical' contact become practical?
- Implementing use and disclosure lockbox rules and notification procedures for electronic records

Enhanced Access and Audit capabilities:

- Use of 'On Line Agreements' for all electronic systems access
- Improved need-to-know (location- and role-based) access controls
- Lifecycle management of access privileges

Training And Education:

- Reaching 8,000+ staff: via department in-service presentations, online self help, orientation, nursing retraining and systems training
- Application to physician credentialing
- Maintaining consistency between policy and procedures

PHIPA "Lockbox"

- **Ethical Premise**
- **PHIPA Provisions**
- **Sunnybrook Policy Overview**
- **Sunnybrook Procedures Overview**
  - Administrative Impact Issues
  - Locking the record
  - Unlocking / Overriding a lock
- **Clinical Impact Issues**

PHIPA "Lockbox"

Ethical Premise

'Consent without ability to withhold/withdraw would be meaningless'

- Consent is not always required
  - Permitted or required C/U/Ds (i.e. not requiring consent) are numerous in PHIPA
  - Based on practicality and balance of cost/benefit
- Where consent is required in a hospital setting, it may be either:
  - Assumed implied based on current or previous presentation for treatment or 'reasonable' notice of purpose;
  - Express (positively acknowledged by the individual, either verbally or in writing)
- Presence of consent in a transaction must be apparent: "reasonable notice" for implied consent = weak; documentation for express consent = strong
- Most (all?) privacy frameworks recognize that the provision or presence of consent is conditional on the ability for the individual providing the consent to withhold (before establishing) or to withdraw (after establishing) consent.

PHIPA "Lockbox"

Legal Provisions Summary

PHIPA Lockbox provisions became effective November 1, 2005

- Hospitals are required to accept a written "express instruction" from patients regarding their withdrawal of consent for the use or disclosure of their personal health information beginning November 1, 2005
  - Private physicians (and all other custodians) have been required to do so since November 1, 2004
  - Applies to any future use (within the hospital) OR (disclosure to another care provider or custodian) "for the purposes of providing health care or assisting in providing health care to the individual".
- A lockbox is not effective for uses/disclosures that:
  - Are required by law (e.g. gun shot reporting, registry disclosures, MOH reporting), or permitted by law (e.g. administrative uses, research without patient contact);
  - Require written consent (e.g. disclosure to an insurance company)
- A lockbox can be 'overridden' to avoid risk of serious bodily harm.

PHIPA "Lockbox"

Legal Provisions

Referenced Sections of PHIPA enabling the lockbox:

- **S. 20(2):** Implied consent may be assumed for C/U/D during the provision of healthcare to the individual…unless the custodian is aware that the individual has expressly withheld or withdrawn consent
  - All other C/U/Ds are either required/permitted without consent, or are subject to express consent
- **S. 37(1)a**: Directly or indirectly collected information may be used based on implied consent **for the purpose for which it was collected** unless the person "expressly instructs otherwise";
- **S. 38(1)a:** Information may be disclosed based on implied consent for the purpose of providing healthcare to the individual unless the person "expressly instructs otherwise";

PHIPA "Lockbox"

Legal Provisions

Referenced Sections of the Act enabling the lockbox override:

- **S. 40(1):** "A health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons."
  - Disclosing custodian may be in a poor position to judge necessity – reliance would be on the requestor's judgment – accountability?
- Note: no apparent equivalent provision for 'use to eliminate significant risk…':
  - Agent use ≠ circle of care disclosure, although both may assume implied consent and may be subject to a lockbox
  - Presumably 'elimination of risk' rationale might apply to any care provider or care provision – in practice, override will likely apply to use as well
  - Is there a professional/legal obligation to use all information in the custodian's possession, whether locked or not? ➔ Obligation would presumably override the lock as a "required use" without need for 'eliminating serious bodily harm'

PHIPA "Lockbox"

Sunnybrook Policy and Procedures Overview

Sunnybrook Privacy Policy allows for withdrawal of consent:

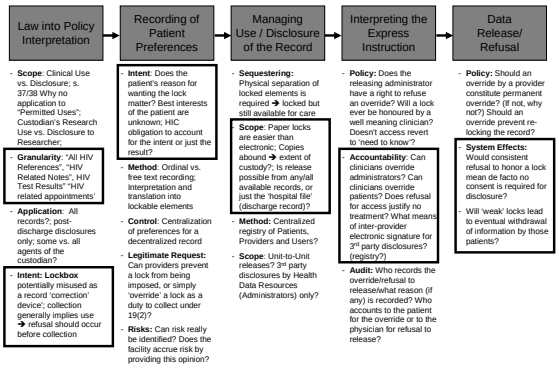
- "In circumstances where the consent of the individual is required for the collection, use or disclosure of personal health information, the individual may withdraw the consent, whether the consent is express or implied, by providing written notice to Sunnybrook's Privacy Office. The withdrawal of consent will not have retroactive effect."

Practical Considerations:

- Sunnybrook continues to review with peer providers to align policy and procedures; consensus on procedures is robust enough for legal compliance and "reasonable efforts" implementation at this time.
- Decentralized record keeping and 'copies' present significant hurdles.
- Emerging MOHLTC eHealth systems are now including lockbox features (e.g. ODB Emergency Drug Profile Viewer)
  - Implementation can be inconsistent with established requirements
  - Sunnybrook Privacy Office monitors emerging systems for best practices

"Lockbox" Administration and Implementation Issues

Sunnybrook Privacy Office – Jan/06



PHIPA "Lockbox"

Sunnybrook Locking Procedures

Sunnybrook accepts written patient requests for a 'lock' on paper charts (see locking flowchart):

- "Request for Lock" forms, patient brochure, locking procedures and staff FAQ are in place – 2 locks have been implemented to date.
- Discrete elements only: Single items; date-to-date encounters; entire chart
- Electronic Chart (EPR) locking process will follow once paper process is stable – scope and limits of 'custody and control' require further definition

All lockbox requests will be reviewed by Privacy Office and Health Records Management on a case-by-case basis:

- Patient must be legally capable of withdrawing consent:
  - Patient or SDM only
  - Mentally capable of appreciating risks of locked information
- Patients will be offered a review of their request with a member of Sunnybrook medical staff in order to understand the risks/benefits of locking information and to assist them in identifying appropriate items to lock.

PHIPA "Lockbox"

Sunnybrook Lockbox Override Procedures

Sunnybrook clinicians may override a lockbox for direct care purposes (see override flowchart):

- Notice of a lockbox is clearly indicated on the hospital file
- Override is possible where the information is required "for the purposes of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons'. PHIPA s. 40 (1).
- Override is 'self-service' for Sunnybrook internal use; 3rd party requestors will be notified of the presence of locked items before Sunnybrook discloses information
- Overrides are subject to retrospective audit

Lockbox is not effective in preventing permitted or required uses or disclosures under PHIPA:

- Sunnybrook administrative uses (quality of care, planning, etc.)
- Education and teaching
- Approved research not requiring patient contact
- Required disclosures: Gunshot; Trillium Organ Donations; s. 39/45 reporting (CCO; CCN; CIHI, etc.)

LOCKBOX NOTICE

SECTION(S) OF THIS CHART HAVE BEEN REMOVED AND PLACED IN A SEALED ENVELOPE IMMEDIATELY FOLLOWING THIS PAGE AS REQUESTED BY THE PATIENT/SUBSTITUTE DECISION MAKER.

IF YOU ARE INVOLVED IN TREATING THIS PATIENT AND/OR YOU REQUIRE ACCESS TO THE LOCKED PORTION(S) OF THIS CHART FOR ONE OF THE FOLLOWING PURPOSES:

- To eliminate or reduce a significant risk of serious bodily harm
- For the purpose of examining, assessing, observing or detaining the client under the Mental Health Act
- Upon receipt of Court Order, Search Warrant, or other Order mandating release of information
- Where the patient authorizes release of locked portion of record
- Other legally required uses or disclosures

CAREFULLY READ AND COMPLETE THE FORM ATTACHED PRIOR TO OPENING THE ENVELOPE

FOLLOWING YOUR REVIEW OF THE INFORMATION, RESEAL THE ENVELOPE (SEALS INCLUDED INSIDE ENVELOPE) AND RETURN CHART TO HEALTH DATA RESOURCES

PHIPA "Lockbox"

Clinical Impact Discussion

1. **Custodians are required to identify <u>potential</u> patient incapability to access their file or to withdraw consent:**
   - Based on <u>previous incapability</u> as may be indicated in hospital file (e.g. indication of a prior psychiatric encounter or prior designation of clinical decision making ability to a 3rd party).
   - Indication of incapability ought to trigger a <u>clinical review</u> by 'most responsible physician'.
   - Notification to patient of declined request - by same physician?
2. **Identifying and describing the risks of locking a record:**
   - Brochure can describe some <u>generic risks</u> of locking records.
   - What other risks (e.g. financial) can or should be listed?
   - Clinical review with patient is optional – all requestors to date have refused.
3. **If clinical review is requested by patient:**
   - How to identify the 'best' clinician for this?
   - What additional risks should a clinician be identifying or disclosing to the patient? Should these be captured in the chart?
   - What liability (if any) does a clinician or Sunnybrook accrue in explaining risks?
     - Likely none, per PHIPA s. 65 and 71(1) – waiting on the 1st case!

PHIPA "Lockbox"

Clinical Impact Discussion (cont'd)

4. **At the point of care – re: clinician consideration to override a lockbox:**
   - What situations or criteria constitute "prevention of serious bodily harm"?
   - Does the lockbox nullify the <u>traditional care provider trust relationship</u>?
   - When would a clinical encounter not require all 'available information'?
   - Does a care provider or clinician accrue any additional liability based on their decision to either override <u>or not override</u> a lockbox?
   - Where the patient may be consulted at the point of care regarding the presence of a lockbox:
     - What are the criteria for a clinician opting to not treat a patient who refuses to rescind a lockbox?
     - What are the clinical obligations for a clinician who refuses to treat based on the presence of a lockbox?
5. **Other Clinical Impacts?**

Presentation Agenda

1. **Organizational Privacy Issues**
2. **Privacy Policy Development & Implementation**
   - **Lockbox Overview**
3. **Towards a Security Framework for Healthcare**

Security

Proposed Privacy and Security Framework

Principles: Legal Obligations and Industry Standards
(PHIPA, PIPEDA, M/FIPPA, CSA Model Code, ISO 17799/27799, IHE, HIPAA, …)

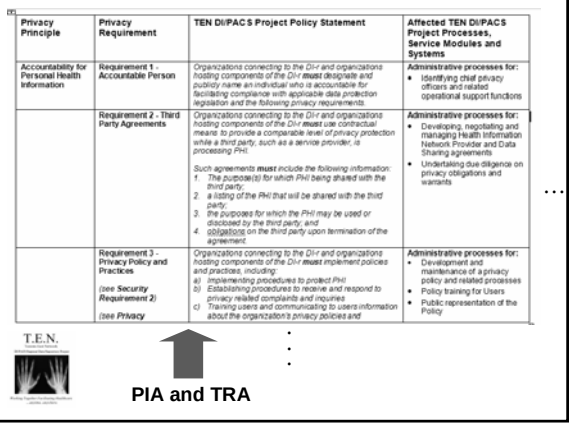
Requirements - Selected Accountabilities and Process

PIA and TRA: Risk Awareness and Analysis

Policy: Avoid, Transfer, Mitigate

Deliverables: Administrative and Technical Processes, Services and Systems

Tracking: Performance Measurement and Management



Privacy Principle	Privacy Requirement	TEN DI/PACS Project Policy Statement	Affected TEN DI/PACS Project Processes, Service Modules and Systems
Accountability for Personal Health Information	Requirement 1 - Accountable Person	*Organizations connecting to the DI-r and organizations hosting components of the DI-r **must** designate and publicly name an individual who is accountable for facilitating compliance with applicable data protection legislation and the following privacy requirements.*	**Administrative processes for:** • Identifying chief privacy officers and related operational support functions
	Requirement 2 - Third Party Agreements	*Organizations connecting to the DI-r and organizations hosting components of the DI-r **must** use contractual means to provide a comparable level of privacy protection while a third party, such as a service provider, is processing PHI.* *Such agreements **must** include the following information:* *1. The purpose(s) for which PHI being shared with the third party;* *2. a listing of the PHI that will be shared with the third party;* *3. the purposes for which the PHI may be used or disclosed by the third party; and* *4. obligations on the third party upon termination of the agreement.*	**Administrative processes for:** • Developing, negotiating and managing Health Information Network Provider and Data Sharing agreements • Undertaking due diligence on privacy obligations and warrants
	Requirement 3 - Privacy Policy and Practices *(see Security Requirement 2)* *(see Privacy*	*Organizations connecting to the DI-r and organizations hosting components of the DI-r **must** implement policies and practices, including:* *a) implementing procedures to protect PHI* *b) Establishing procedures to receive and respond to privacy related complaints and inquiries* *c) Training users and communicating to users information about the organization's privacy policies and*	**Administrative processes for:** • Development and maintenance of a privacy policy and related processes • Policy training for Users • Public representation of the Policy

…

T.E.N.

PIA and TRA

Security

Proposed Privacy and Security Framework

Challenges:

- **Picking the Right Principles:**
  - PHIPA is a great start, but other Acts apply in an
  - ISO 27799 is better…but is it any more practical than 17799?
- **Achieving all of the Requirements:**
  - CHI lists over 28 Privacy and 53 Security Requirements in it's framework – achievable?
- **Conducting meaningful PIA/TRA:**
  - Experts needed to identify/quantify all of the risks
  - Risk Management is an art: subject to bias and budget
- **Conducting meaningful PIAs/TRAs:**
  - Experts needed to identify/quantify all of the risks
  - Scope grows quickly beyond single systems
- **Selecting the Right Policy:**
  - Public statements of accountability – not everyone will agree with your approach!
  - Policy alone doesn't get the job done: and walking the talk may require revisiting the policy
- **Delivering on Admin and Technical Processes**:
  - Accountability becomes decentralized and requires active management with multiple agents and partners
  - Good News: Healthcare relevant best practices for P&S management are becoming more available

Thank You

Sunnybrook Health Sciences Centre
Privacy Office – privacy@sw.ca

jeff.curtis@sunnybrook.ca
(416) 480-6100 ext. 3538

Public info at www.sunnybrook.ca
"Patient's and Visitors" > "Privacy and Confidentiality"

The re-identification of anonymized records in Ontario
Khaled El Emam (PhD), Associate Professor, University of Ottawa

Bio:
Dr. El Emam is an Associate Professor at the University of Ottawa, Faculty of Medicine and a Canada Research Chair in Electronic Health Information at the University of Ottawa. His research office is at the Children's Hospital of Eastern Ontario Research Institute, where he is leading the eHealth research program. In addition, Khaled is the Chief Scientist at TrialStat Corporation, a company that develops electronic data management systems for clinical research. Previously Khaled was a senior research officer at the National Research Council of Canada, where he was the technical lead of the Software Quality Laboratory, and prior to that he was head of the Quantitative Methods Group at the Fraunhofer Institute for Experimental Software Engineering in Kaiserslautern, Germany. In 2003 and 2004, Khaled was ranked as the top systems and software engineering scholar worldwide by the Journal of Systems and Software based on his research on measurement and quality evaluation and improvement, and ranked second in 2002 and 2005. Currently, he is a visiting professor at the Center for Global eHealth Innovation at the University of Toronto (University Health Network) and at the School of Business at Korea University in Seoul. He holds a Ph.D. from the Department of Electrical and Electronics Engineering, King's College, at the University of London (UK).

Measuring Re-identification Risk

Khaled El Emam
University of Ottawa

Contents
General
Re-id
End

Collaborators

- Sam Jabbouri, Carleton University
- Scott Sams, London School of Economics
- Youen Drouen, Universite Lumiere Lyon 2
- Michael Power, Gowling Lafleur Henderson LLP

These results will appear in the Journal of Medical Internet Research (www.jmir.org)

Contents
General
Re-id
End

Our Scenario

- We assume that there exists a database with PHI and we wish to anonymize it effectively, but not reducing the value of the data by too much
- The first step is to understand the different ways in which this database can be attacked, then we can construct defenses against these attacks

Types of Variables

Contents
General
Re-id
End

- Identifying variables
- Quasi-identifiers
- Non-identifying variables
- Sensitive variables

- HIPAA's methods (safe harbor and limited data set) focus on removing identifying variables and quasi-identifiers to various degrees
- Canadian legislation is not specific on variables to remove

Identifying Variables

Contents
General
Re-id
End

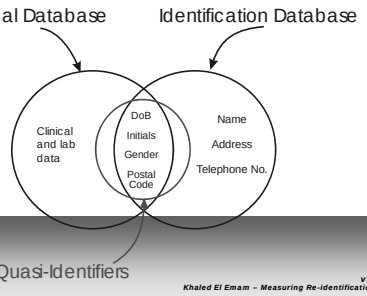
- Can always remove these variables from the database
- In some cases it is important to have values in the data set for the identifying variables
- Can replace these with realistic values randomly: gender correct first names, fake email addresses, realistic SINs, realistic credit card numbers, …

Sensitive Variables

Contents
General
Re-id
End

- These variables can be removed or encrypted
- Sensitive variables make the data valuable for an attacker, therefore the inclusion of such variables in a data set has to be carefully considered

Record Linkage Scenario



Re-identification in US - I

- It is possible to identify 87% of the US population using *{DoB, gender, 5-digit ZIP}* by linking with publicly available information
- About half of the population can be identified by *{DoB, gender, place}* where *place* is the city, town, or municipality where the person resides
- At the county level, 18% of the population can be uniquely identified *{DoB, gender, county}*

Re-identification in US - II

- Voter lists are publicly available in the US, for example. But the Elections Act in Canada puts restrictions on when and to whom voter list information is disclosed
- There are other examples of successful attacks (matching experiment) in the US, Germany, and the UK
- Probability of re-identification depends on what external databases are available – and this will change over time and by jurisdiction

Identification Databases in Canada

Contents
General
Re-id
End

- Once you have constructed an identification database, then it is easy to attack anonymized databases
- We will now look at ways that we can construct identification databases in Canada …

Identification Databases - I

Contents
General
Re-id
End

- We tried to identify public or semi-public population or sub-population databases in Ontario to use as sources with *{DoB, initials, postal code}*
- **Public Data** is available to the general public, for free or a reasonable fee with a reasonable amount of effort to get access to it, without a review by the data holding institution nor the need to sign a confidentiality agreement with the data holding institution that restricts what can be done with the data

Identification Databases - II

Contents
General
Re-id
End

- We interviewed staff at the privacy office (phone) in almost all ministries, interviewed a sample of commercial information brokers, investigated public archives, and sources of genealogical data
- The objective was to identify and if possible obtain public identification databases on Ontario residents

Identification Databases - III

Contents
General
Re-id
End

- Most ministries have a privacy officer who oversees disclosure and enforces privacy and access to information requests
- The privacy offices do not have a comprehensive idea of the data that is being released by their ministries
- Commercial brokers link census data with white pages – age data is very approximate

Professional Groups - I

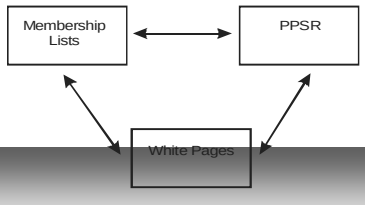
Contents
General
Re-id
End

- College of Physicians and Surgeons of Ontario
- Law Society of Upper Canada
- Professional Engineers Ontario
- College of Occupational Therapists
- College of Physical Therapists
- .....

Professional Groups - II

Contents
General
Re-id
End

We can construct identification databases for specific professional groups



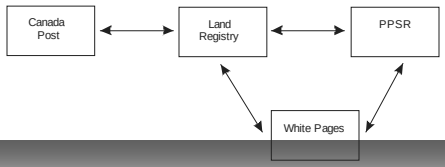
PPSR

Contents
- General
- Re-id
- End

Homeowners

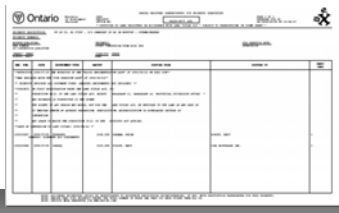
Contents
- General
- Re-id
- End

We can construct identification databases for specific postal codes



Land Registry

Contents
- General
- Re-id
- End



What is the success rate ?

Contents
General
Re-id
End

	CPSO	LSUC
• Ability to get home postal codes (source: PPSR and telephone directory)	60%	45%
• Ability to get practice/firm postal codes (source: CPSO/LSUC)	100%	100%
• Ability to get date of birth (source: PPSR)	40%	45%
• Ability to get gender (source: CPSO/**genderizing** LSUC)	100%	100%
• Ability to get initials (source: CPSO/LSUC)	100%	100%

What is the success rate by gender?

Contents
General
Re-id
End

	CPSO	LSUC
MALE		
• Ability to get home postal codes (source: PPSR and telephone directory)	63%	48%
• Ability to get date of birth (source: PPSR)	45%	48%
FEMALE		
• Ability to get home postal codes (source: PPSR and telephone directory)	49%	40%
• Ability to get date of birth (source: PPSR)	29%	40%

What about attacking a database ?

Contents
General
Re-id
End

- We simulated an attack on a lawyer and a physician database (1% sample)
- If we assume a 1:100 success rate (on average) is our threshold (i.e., if we can identify 1/100 of the people in the database or less then the database is safe) then:
- Safe Quasi-identifiers:
  - [gender], [region], [year of birth] on their own
  - [gender] & [region] combination
- Other quasi-identifiers were found to have a high risk of re-identification
- Results are consistent across both data sets

Policy & Practical Implications - I

Contents
General
Re-id
End

- It was not possible to construct an identification database for the whole population
- It was possible to construct identification databases for sub-populations that can be listed: lawyers, physicians, home-owners

Policy & Practical Implications - II

Contents
General
Re-id
End

- We should not restrict access to data sources, such as the PPSR, because there are legitimate business needs for their existence
- Data sets where any sub-population can be listed (e.g., lawyers, physicians, home-owners) can be re-identified with relatively high probabilities
- It would not be possible to do this with youth because the data sources used do not exist for youth

Policy & Practical Implications - III

Contents
General
Re-id
End

- Researchers/companies may have access to additional databases, therefore data sharing agreements are always necessary
- What we presented here can easily be done in other provinces and territories because the same information is publicly available

Policy & Practical Implications - IV

Contents
General
Re-id
End

- It is important to use more sophisticated anonymization techniques than simple heuristics about what variables to include/exclude
- Avoid publication of membership lists, and if it is necessary the members ought to be notified of the privacy risks
- Implement financial deterrents for the construction of identification databases
- Remove unique members from public lists

Contacts

Contents
General
Re-id
End

Khaled El Emam
kelemam@uottawa.ca
(613) 797 5412

www.ehealthinformation.ca

Privacy Considerations During the Implementation of Electronic Health Records
Glen Geiger, Medical Director, Clinical Information Systems, The Ottawa Hospital

Bio:
Dr. Geiger has an undergraduate degree in Electrical Engineering at the University of Waterloo, and went on to obtain his medical degree from McGill University in 1988. He completed fellowship training in General Internal Medicine at University of Western Ontario in 1992, and then undertook a Masters of Biomedical Engineering at the University of Toronto, completed in 1995.

He has worked on Electronic Patient Record systems for over ten years and has continue to practice medicine as an academic internist.

Dr. Geiger is currently the Medical Director, Clinical Information Systems at the Ottawa Hospital where he is leading the hospital's efforts to implement Computerized Physician Order Entry.

Dr Geiger is a national leader in Health Information Systems implementation. His major areas of interest include:

- Care Process Re-engineering
- Clinical Decision Support
- Patient Medication Safety
- Health Care quality and Outcomes Measurement
- Personal Health Information Privacy

Privacy Considerations During the Implementation of Electronic Health Records: Has PHIPA Changed Anything?

Dr. Glen Geiger
The Ottawa Hospital

November 13th, 2006

Outline

- Applying PHIPA to care delivery: The devil is in the details
  - HIV results
  - Employee Results
  - Psychiatry Notes
  - VIP status
- Applying PHIPA elsewhere in the enterprise
- The Sinister Case of HO-002
- Personal Recommendations

Maintaining Privacy while delivering health care

HIV Results

HIV Results

- As of November 1st, 2006, HIV results will now upload from the laboratory system into the Electronic Patient Record at the Ottawa Hospital
- This information had previously been excluded as the result of a decision making process lost in the 'mists of time'
- The decision to include this information was ultimately taken by the Medical Advisory Committee

Reason to include HIV

- The text of Discharge Summaries and some clinic notes already available through the EPR contained information about the patient's HIV status
- Clinic encounters with HIV specialists could not be systematically hidden because these physicians also have a non-HIV practice
- The medication lists are available online through the EPR and include the display of Protease inhibitors and anti-retro-viral drugs.
- Times have changed

Employee Results

Exclusion of Employee Results from the EPR

- It has been the practice of Occupational Health, to register staff members against special outpatient accounts so that their results do not populate the EPR
  - This has been done through paper requisitions with special stamps to identify them as Occ Health requests
  - Typical tests would include MRSA screening and HIV testing after a needle stick injury

Issues arising from special handling of Employee Results

1. In the event of a needle stick injury, we are going to require the patient to be tested for HIV and will record their result in the EPR
   - But our staff get special treatment, we exclude their results from the EPR
2. What do we do when staff members become patients?
   - Clinicians caring for them will be unable to see their HIV results and MRSA status
   - This creates the potential for substandard care and liability

Treating the Personal Health Information of staff differently from that of everyone else creates two classes of citizens: That's wrong!

Corollary: If our own staff don't trust us to keep their information private, why should anyone else?

Psychiatry Notes

Psychiatry Notes

- It has been the practice of many hospitals and psychiatrists to segregate patient's psychiatric histories and inpatient encounters from other personal health information, citing the Mental Health Act as justification
- At the Ottawa Hospital, inpatient psychiatric encounters are not readily viewable. The user must specifically remove a filter in order to view all encounters
  - At this point the user is warned about the seriousness of breaching patient confidentiality
  - The user gets the same warning if he or she tries to open the Psychiatry inpatient location roster

Issues Relating to Psychiatric Notes

1. The Personal Health Information of a patient seen in the Emergency Department with a drug overdose is accessible to all
   - While the patient is treated for the overdose in the ICU and the acute care med/surg units, no special protection exists
2. If a patient with a psychiatric diagnosis is sent home without ever being admitted to psychiatry, no special restrictions are placed on the encounter record or the discharge summary
   - But if the patient is accepted in transfer to the psychiatric ward, the encounter is marked as privileged

Treating the Personal Health Information of patients seen by psychiatry, differently from that of everyone else creates two classes of citizens: That's wrong!

Corollary: The tools to restrict access to such records are clumsy and ineffective.

VIP Patients

VIP Status

- Some patients are flagged in the Registration System as VIPs
- This sets a warning flag in the EPR so that clinicians accessing the record are alerted to the sensitive nature of the record

Issues arising from the VIP flag

- Who do we set the flag for?
  - Politicians
  - Celebrities - that we've heard of…
    - ✓Sean Connery
    - ✖K-Fed who? Beckham who?
  - Anyone? Everyone?
- Maybe we should make all of our staff members VIP's
  - Maybe we should at least give all of our staff members the option to designate themselves as VIPs
  - Does VIP status lose its meaning if thousands and thousands of people acquire this attribute

Maintaining Privacy while measuring quality and doing research

"…for after the Seventh Seal was opened I raised my eyes and beheld vast rivers of patient information flowing in all directions…"*

*Revelation 8:1

TOH Physician Advisory Committee

- Meets bimonthly
- Every meeting is completely taken up by physicians asking for approval for new clinical databases. The justifications are always the same
  - To carry out research on quality
  - To deliver better care
- The deliberation is always the same
  - Do we have the resources to address the request?
  - The question is never, "Does your request to collect, use and disclose patient information over-ride our obligation to respect patient privacy?"

The Thirst for Data

"Such was the Spaniard's insatiable demand for gold, that the Aztecs came to believe that Cortez and his men needed it to live…"

- Clinicians and scientists today behave as if they have a right to acquire patient information
  - Any suggestion to the contrary produces apoplexy and warnings that the health care system will crumble (or at least their academic careers) if they can't have this data.

"I've got a friend in the lab who gets me data…"

The Sinister Case of HO-002*

*This information comes from the HO-002 report prepared by Ann Cavoukian as Information and Privacy Commissioner of Ontario.

Details of the Incident

- Patient (Complainant) admitted to the Ottawa Hospital, identified from the outset that she was concerned that her ex-husband (lets call him Boris), an employee of the hospital, might use her health information in their ongoing divorce proceedings and custody battle
- Ultimately, the ex-husband did indeed confront the patient with detailed knowledge of her medical condition and recent treatment, prompting the complaint
- The patient contacted the Ottawa Hospital Privacy Office, prompting them to set the VIP flag on the patients records

The Investigation

- The Ottawa Hospital was able to audit the Electronic Patient Record System and show that the ex-husband's girlfriend, a nurse at the hospital, lets call her Natasha, accessed the patient's information multiple times.
- The hospital confirmed that there was no care relationship that could explain this access
- Internal disciplinary action was taken against both employee's
  - Natasha was suspended without pay for four weeks
  - Boris was suspended without pay for 10 days

Findings: What went right

- Staff in the hospital noted the patient's concerns
- Steps were taken to ensure that the patient's ex-husband was not scheduled to work in areas where the patient would be
  - The IPC acknowledged that the hospital worked pro-actively to address the physical security of the patient in this manner
- The VIP flag was set after the complaint to the Ottawa Hospital Privacy Office
- The hospital was able to audit and identify the inappropriate access

Findings: What went wrong

- Although the hospital was pro-active in addressing the patient's physical security, they were woefully lax in addressing the patient's privacy
- The hospital's existing policy "Protecting Patient's Privacy" was not followed…
  - VIP flag not set till after complaint
- The nurse continued to access the patient's information for a further 3 weeks after the VIP flag was set
  - Hospital did not confront the staff member because they were following their complaint procedure with Human Resources and the union
  - Hospital did not disable access by the nurse

The patient noted in her complaint to the IPC that following notification of the Ottawa Hospital's Privacy Office, "illegal access to [the complainant's] personal health information continued unabated…," for an additional three weeks…

The hospital advised that during the course of its investigation, the nurse did indeed ignore the VIP flag and accessed the complainant's electronic health record on three further occasions

Is there a theme emerging here?

- Special security features to protect HIV status will not achieve the desired effect
- Special security for psychiatry encounters does not achieve the desired effect
- Just plain excluding employee information to ensure their privacy is a 'dicey' proposition
- The VIP flag works, but execution has been flawed and the question of who should be identified as a VIP remains

The answer lies <u>not</u> in increasing electronic security measures…building a fortress around personal health information…

but rather, through vigorously reinforcing the culture of respect for patient privacy

"Hospitals must ensure that they not only educate their staff about the *Act* and information policies and practices implemented by the hospital, but must also ensure that privacy becomes embedded into their institutional culture."

Ann Cavoukian, HO-002

Personal Recommendations to Enhance the Culture of Privacy

Recommendation One

- Ongoing auditing of Clinical Information access and active follow-up
  - Users should expect routine calls to check up on their actions
  - It would not take many such calls across the user community to establish a zero tolerance attitude
- Ongoing efforts to find ways to filter suspicious events out of the massive audit logs. Focus on…
  - Single patient look-up events
  - Change of location events
  - Remote access events
  - Large access events

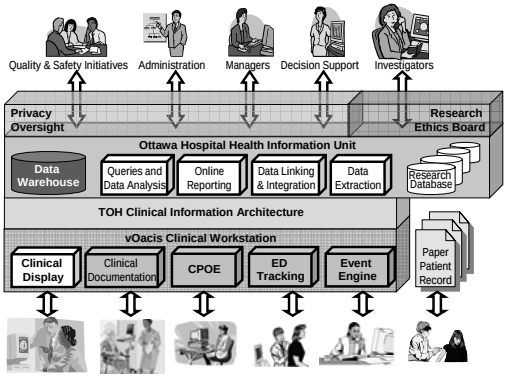
Recommendation Two

- Establish convincing oversight for all registries and disease management/tracking/quality monitoring databases
- Stakeholders involved with such databases should understand and acknowledge that…
  - Using patient information is a privilege
  - They will be held accountable for misuse or disclosure
  - Maintain audit trail of which patients are within the scope of the database

Recommendation Three

- The Research Ethics Board should be expected to…
  - Define the scope of the researcher's data collection, use, retention and release in detail…
    - Which data for which patients?
    - How long can the information be held? (can't be indefinite)
    - How can the information be shared with other researchers or research sponsors?
  - Request description of data security measures, maintenance of passwords, etc.
  - Establish final accountability of the researcher including signed acknowledgement
  - Maintain an audit trail of approved research requests

Information System Stakeholders



Conclusions

- Yes, things have improved following the introduction of PHIPA
  - The establishment of a legal framework and complaints process for breaches of privacy will focus the attention of Health Information Custodians on this issue
  - Orientation programs for employees are placing increased emphasis on privacy
- We still have a way to go…
  - Respect for patient privacy needs to become second nature for clinicians and researchers. This would be enhanced through…
    - An active process of auditing and follow-up for clinical access
    - An active process of oversight for research, registries and quality measurement activities

Technology Aids Privacy Compliance in Healthcare

Michael Gurski, Bell Security Solutions

Abstract:
Privacy in the healthcare sector has moved to the executive management agenda. The reason for this is health privacy legislation that introduces the patient as an actor in the identity management schema and a controller of their personal health information (PHI) under different circumstances. With the evolution to electronic health records, regional health information data centres and the ready access to PHI needed for effective and efficient healthcare privacy technology solutions need to be designed into healthcare systems. This talk will explore the challenges to building privacy into healthcare systems as well as some solutions and promising lines of privacy enhancing technology research. The areas covered in the presentation include technologies that solve patient consent management and lock box functionalities, user centric identity management that provide patient controls, as well as privacy enhancing technology research that will have commercial interest in the health care space.

Bio:
Mike Gurski is the Director of the Bell Privacy Centre of Excellence and the Privacy Strategist for Bell Security Solutions Inc. (BSSI), Canada's premier security and privacy solutions provider. He is an active member of the International Security Trust and Privacy Alliance working to develop ISO standards for privacy. Prior to joining BSSI, he chaired an international Privacy Enhancing Technology Testing and Evaluation Project to develop privacy evaluation standards. He also acted as the Chief Technology Advisor at Ontario's Information and Privacy Commission. He is on the Board of the Privacy Enhancing Technology (PET) Research Workshop, and chairs the international PET Executive Briefing Conference. Mike is also a founding member of the "The Privacy Network", a knowledge exchange network to link various privacy communities in Canada.

Building Privacy and Security Technology into Health Care Environments.

The Preconditions & Solutions

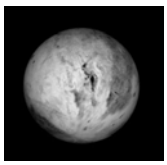
Mike Gurski
Privacy Strategist
Bell Security Solutions Inc.
Head: Privacy Centre of Excellence
November 13, 2006

Our Agenda

- Setting the Context:
  - **Dispelling the misconceptions around Privacy and Security**
- The Necessary Foundation Stones for introducing privacy protections
- The Role of Privacy Technologies in Health Care
  - Addressing the Perceived Barriers to Introducing Privacy Technologies
  - The Argument for Introducing Privacy Technologies
  - Privacy Solutions for various environments
- Discussion

A Privacy Quiz

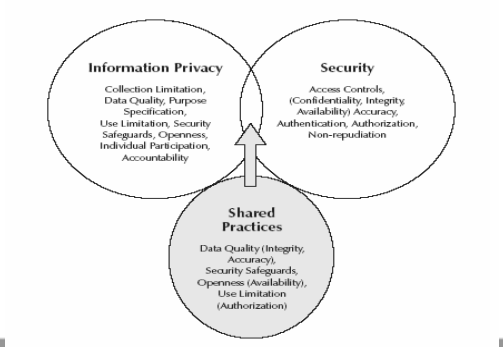
- 2003 EL_{61}
- Sedna
- Orcus
- Quaoar
- Varuna
- Ixion
- Vesta
- Pallas
- Pluto



Privacy & Security Misconceptions

- The strings of control.
- Policy/Technology.
- The Language Barrier
- Downside of Follow the leader.
- Does anyone really care?
- http://www.ipc.on.ca/images/Resources/sec-priv.pdf

The Privacy Security Venn Diagram



The Argument for Introducing Privacy Technologies

- 'Getting Privacy Right' will be Key to the Success of the EHR
  - Richard Alvarez , President & CEO, Canada Health Infoway
- **"Privacy by Design: Don't Make Privacy An Afterthought – Build It In"**

  Ann Cavoukian, Ph.D.

  Information & Privacy Commissioner/Ontario

Privacy by Design is trademarked by DataPrivacyPartners

The Role of Privacy Technologies

- Are filing cabinets scalable?
- How can privacy technologies increase health care efficiencies?
  - Before breach
  - After breach
- What technologies can you introduce, from the doctor's office to the EHR?

Laying the Foundation

- The Prerequisites to Introducing Privacy Technology Solutions
  - High Performance Privacy Organization
    - Roles & Responsibilities
    - Organizational Design
  - Privacy Strategy with Measured Outcomes
  - Enterprise Privacy Architecture
  - Privacy Policies & Procedures
  - RFP process that incorporates specific privacy functionality requirements
  - Enterprise PIA's, as opposed to project specific PIA's
  - Integrated TRA/PIA capability and feedback to systems design
  - Role of PIA's in building privacy into an enterprise

What is a High Performance Organization?

- **1** - The right people are the origin and end of the high-performing organization.
  - Aligned, teamed, energized, capable, and pioneering people create high-performing organizations, and attracts, nurture, and develop these people..
- **2** - People at high-performing organizations are guided by a single imperative:
  - *to maximize public service through learning*.
  - They focus on leveraging learning into perfecting the achievement of the Organization's **intent**.
- **3** - All elements other than people are optional.
  - The traditional trappings of organizations (structure, strategy, systems, procedures, equipment, tools, and facilities) contribute nothing to its success except as they serve and are used by its people.

Steps to a High Performance Privacy Organization.

- Educate leadership and staff on privacy
  - Require privacy expertise in management and staff
- Uncover and remove the obstacles to high-performance and realize the opportunities for advancement/leadership
- Engage your people in service improvement activities that align to your Organization's Intent, team them in making change, stimulate their energy with opportunities to make a difference, enable them with knowledge and skills, and encourage them to see privacy in new ways
- Elevate your people's ability to generate new ideas, acquire privacy knowledge rapidly, and transfer it efficiently across the organization
- Conduct renewal sessions that reflect on your progress, extract learning, and fold that learning into increased privacy successes.

Lessons on an Enterprise Privacy Strategy?

- A Lesson From Peru:
  - The Shining Path Terrorist Organisation
    - The Dentist, the Ballerina, and Abimael Guzman
    - The tragedy of an aversion to high performing organizations.
- A Lesson from the Federal Government:
  - Is the Social Insurance Number a file tag or an identifier?
  - Is there a federal Identity Management Strategy or Policy?
- A Lesson from Quebec:
  - Minister Gautrin, IDM, My Citoyen, Cliqsecur, Privacy
- A Local Lesson
  - You know better than us.

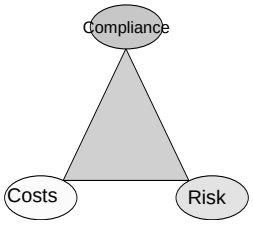
Components of an Enterprise Privacy Strategy.

- Walk before your fly:
  - A lesson in e-mail encryption
  - Privacy Acculturation
  - Strategy Articulation (applying risk management techniques)
  - Planning and Implementation
  - Missionary Work
- Achieving Cruising Altitude:
  - Ongoing education and training
  - Periodic reinforcement of importance of privacy
  - Operational reviews and Audits
  - Strategy and Plan review

Privacy Strategy Content

- Your Strategy should set out the direction for your Enterprise Privacy Architecture
- Consider enshrining privacy architecture principles in policy
  - First you need an enterprise privacy architecture
- Every HIC should have a PIA policy as part of its Strategy
- Policy should be specific enough to ensure that its objectives are achieved and measurable, but broad enough to permit flexibility in its application
  - Needlessly prescriptive privacy policy creates resistance
- Recognize that Policy is not enough.

The Privacy (and IM) Value Proposition



- What this teaches us.
  - Integrating Risk Assessment into PIA's is critical.
  - Understanding the costs for compliance and non-compliance needs to be articulated
  - Compliance is both to PHIPA and patient values and expectations

Risk management

- Privacy planning is more effective if approached from a risk management perspective than a legal compliance perspective
  - Risk management permits the efficient allocation of resources
  - Legal compliance requires the allocation of resources to all compliance issues regardless of risk
- The PIA is the primary risk assessment tool but is an orphan and needs to expand to incorporate threat assessments
  - Ensure that PIAs don't become bureaucratic exercises in which the completion of the PIA is more important than its conclusions
  - Ensure the PIA drives back into the project management cycle.
  - External expertise should be brought in to do PIAs only if the project is unusual or complex enough that internal expertise is inadequate.
  - Internal expertise should be adequate for most PIAs in a High Performing Organization.

The Barriers for Privacy Technology Solutions

- No legal requirements for using technologies
- No funding source
- No off the shelf solutions
- Legacy Systems
- Limited ramifications of privacy breeches
- A privacy architecture with options
- The role of RFP's
- The role of Privacy Impact Assessments

I cannot do it, Captain, I don't have the power. We're on Impulse Engines only.

Privacy Technology Assumptions going in.

- In so far as technology is concerned, privacy and security must be considered in the same breath; it is not a balancing act, this is not the Cirque de Soleil
- Like security, privacy must be automated to be effective in high-volume, transaction oriented information systems!
- Privacy automation remains in its infancy, but sufficient progress is being made to justify its inclusion in strategic planning
- The use of privacy expert systems, especially for privacy impact assessment, is come of age.
- The enterprise privacy architecture guides information systems development and redevelopment

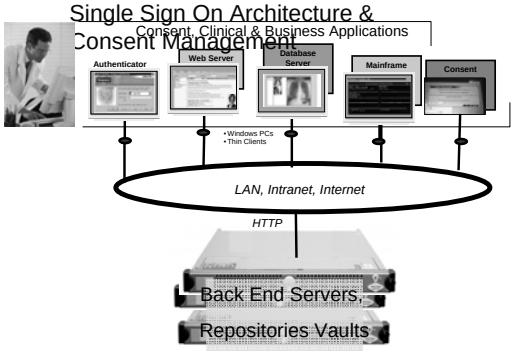
The Privacy Technology Pieces: Conceptually

- Authentication & Authorization
- Privilege Management
- Consent Management
- Audit Trail Management

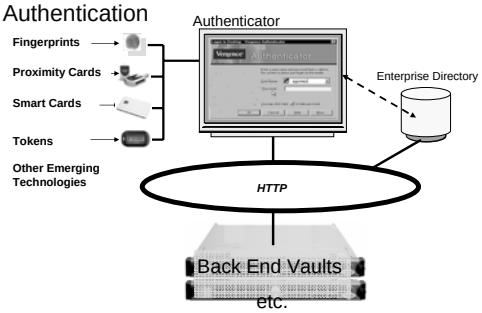
The Privacy/Security Challenge:

How do you manage health information in a privacy protective way that actualizes PHIPA and ensures the security of EHR's?

Introduce Real Time Provisioning, Single Sign On Architecture & Consent Management



Introduce Access Controls: Strong Authentication



Benefits of Authenticator Solution

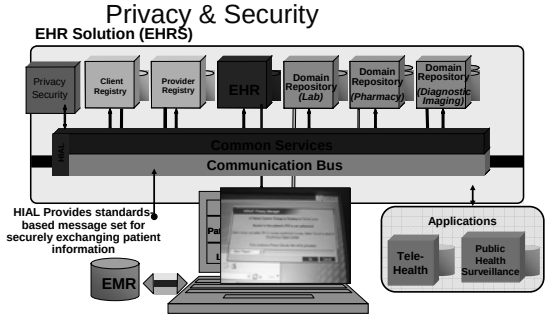
- Control access to shared workstations, PCs and thin client devices, limiting entry to only authorized users.
- Deliver strong authentication via built-in device support for proximity and biometric authentication mechanisms.
- Optimize investments in existing password infrastructures, verifying users against Microsoft® Active Directory®, Novell Directory Services® eDirectory®, Sun® SunOne® or any LDAP directory.
- Strengthen security on PCs and shared workstations through uniform authentication, a secured screen-save, on-demand re-authentication, and others.

Decrease caregiver frustration and improve system use.

Provide Strong Privacy Auditing Solution

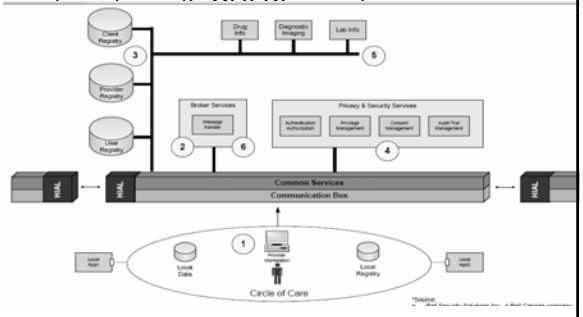
- The P&S solutions logs audit messages from all sources following IHE's ATNA security profile. Messages include:
  - PHI access, modification, disclosure (e.g. emergency override access)
  - administrator access to audit logs
  - security incidents
  - privacy events
  - security events
- Audit logs in a secure, centralized location to prevent tampering (see Security).
- The solution will provide a mechanism for digitally signing audit messages at the source.
- All audit messages generated under context management can be stored in the central repository.

Tying it all together plus Privacy & Security



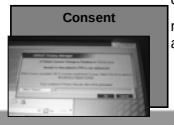
An interoperable EHR captures all key clinical data on one screen (role-based)

Start with a reference Architecture that



Consent Solutions

- Consent Solution consent directives (lock box)
  - express consent
  - personal health information (PHI) access/ correction requests
  - complaints
  - disclosures
  - Security



- recording of patients' consent directives / preferences
- managing access to locked PHI
- emergency override access to consent directives and PHI
- flagging the privacy administrator when emergency override has been activated
- auditing access to consent directives and PHI

recording emergency overrides as disclosures

Controlling access to locked PHI

- By using context management, we can control user access to PHI at various levels of granularity, based on context elements:
  - patient ID
  - user ID
  - encounter number
  - order number
  - as determined by hospital

Conclusions:

- Focus on the people in your organisation first and foremost
- Use privacy strategies and policies to support their performance
- Create a privacy learning environment, reward privacy expertise
- Pilot the new high performing privacy organization
- Introduce Privacy & Security Technologies in the Right Context
- Shift to designing privacy in from the get go.

And in case you are Interested…

Bell Security Solutions Inc./Privacy Centre of Excellence

- Provides end-to-end privacy solutions:
  - Integration of privacy Info and Infra structures (strategy and technology)
  - Enterprise-focused solutions
  - System Integration support for BSSI Security Solutions
  - Professional Management Services
- Directs $1.5m privacy technology research in 06 for commercialization:
  - Adhoc Wireless Networks in Healthcare Environments
  - Health Informatics for 07 with McMaster and others
- Demonstrated Thought Leadership
  - Established ThePrivacyNetwork.org (w/ UoT, Microsoft, Gowlings)

Discussion

Contact Information

Mike Gurski

Privacy Strategist

Head: Privacy Centre of Excellence (PCE)

Bell Security Solutions Inc

905-751-4310

mike.gurski@bell.ca

Title of slide

Subtitle

- First text level
  - Second text level
    - Third text level

Privacy Enhancing Technologies: A Microsoft Perspective
Steve Heck, Privacy Officer, Microsoft Canada

Abstract:
While Health Practitioners, Project Managers and IT Professionals fully appreciate that respect for privacy principles is a foundational requirement for any health project, implementing privacy safeguards remains a challenge. As the practice of privacy becomes better understood, so do the privacy safeguards instantiated through policies, procedures, people readiness and products become better understood. Join Steve Heck, Privacy Officer for Microsoft Canada, as he discusses technologies that enhance privacy and the processes that can be used to ensure that they are implemented correctly.

Bio:
As Group Manager, CRM / Privacy Officer, Steve oversees Microsoft's Campaign Operations, Data Quality, Analytics, and Process Management Teams as well as holding responsibility for all Customer Privacy related issues. Steve is a longtime member of the CRM community in Canada having spent over 13 years in the information and marketing arena.

Steve has been involved in Privacy industry in different capacities dating back to the introduction of Bill C-6 and its integration into the financial services industry in the late 1990's. Steve's ownership for customer data and related business functions has put him front and center on Privacy issues that continue to evolve as customer data flows through all aspects of our economy.

Steve took over responsibility for the Privacy Office at Microsoft Canada in December 2005 given his privacy experience and his stewardship responsibilities for the use and protection of customer data at Microsoft.

Since then, Steve has focused a great deal of effort to implement Microsoft Corporation's Global Privacy Policy within Microsoft Canada ensuring that MS respects both Canadian Privacy laws, as well as our Customer's preferences and expectations.

Privacy Enhancing Technologies: A Microsoft Perspective

Steve Heck, Privacy Officer – Microsoft Canada

Outline

- **Privacy Officer's Perspective**
- **Microsoft's Experience**
- **Privacy Enhancing Technology**
- **Looking Forward**

Privacy

"the right to control access to one's person and information about one's self."

Privacy Commissioner of Canada, speech at the Freedom of Information and Protection of Privacy Conference, June 13, 2002

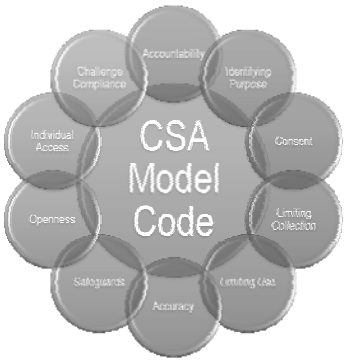
3

Technology & Privacy

- Privacy compliance is a system of:
  - People
  - Knowledge
  - Processes
  - Policies
  - Technology
- Technology facilitates, streamlines & constrains the other components

'A fool with a tool is still a fool'

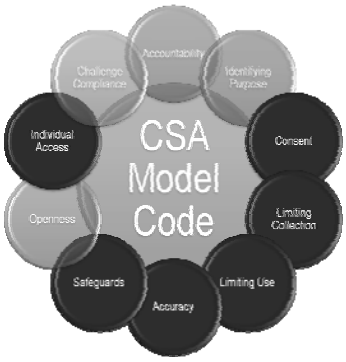
CSA Model Privacy Code



5

http://www.csa.ca/standards/privacy/code/Default.asp?language=English

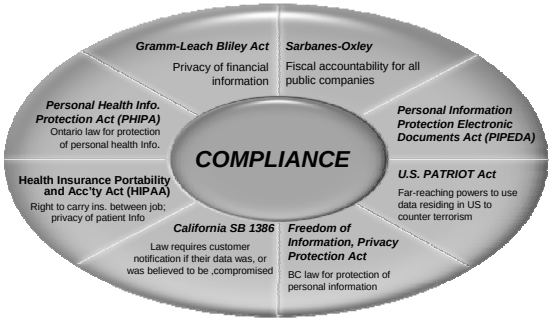
CSA Model Code – Technology Reliance



6

http://www.csa.ca/standards/privacy/code/Default.asp?language=English

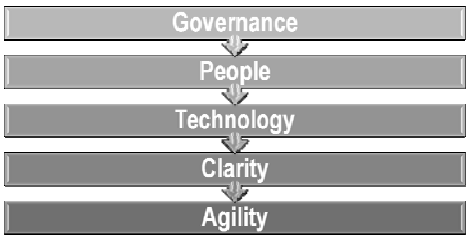
The Context Of Privacy Compliance



Impact of Non-Compliance

Privacy Challenges

Microsoft's Experience



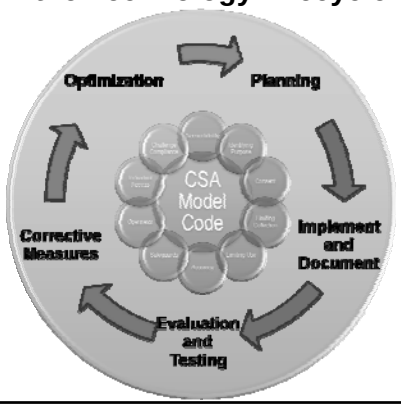
Governance

- Executive Commitment to Privacy
- Privacy Officer Access to Senior Management
- Define Accountability
  - PCO is the Privacy SME / Consultant / Liaison / Auditor
  - Organizational units own the risk

People Enhancements

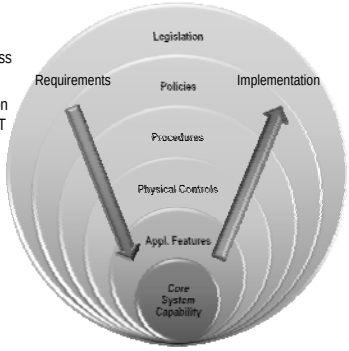
- Use the Technology You Have
  - Hyper-links, access permissions, limiting collection, file transfer processes, password protection, e-mail policies
- Define Standard Processes
- Educate
  - What is privacy?
  - What is their responsibility?
  - Why is it important?
- Design Applications with Privacy in Mind
- Drive for Simplicity & Clarity

Privacy in the Technology Lifecycle



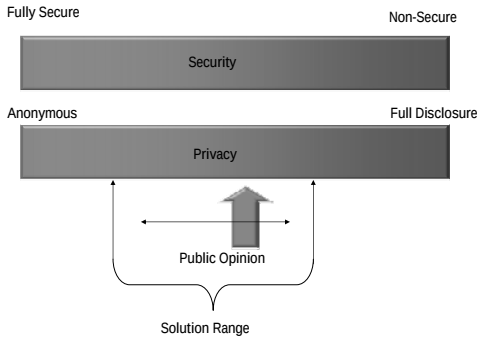
Implement Privacy Defence in Depth

- Engage the entire organization for success
- Allows for the allocation of controls outside of IT
- Supports a multidisciplinary approach

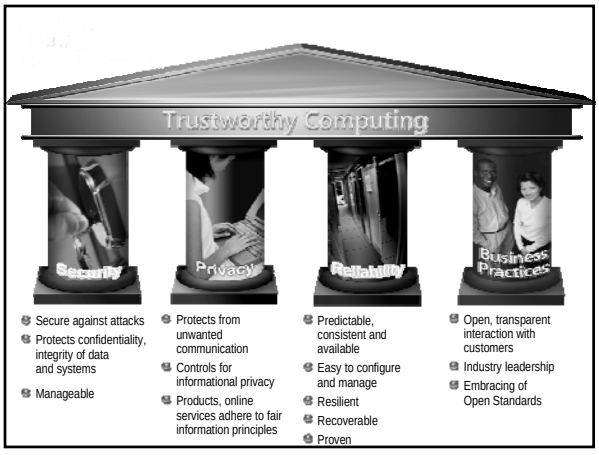


Clarity: Layered / Short Notice Disclosure

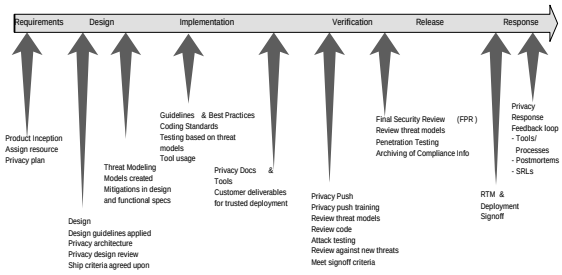
Privacy Agility



Microsoft's Commitment to Privacy



Development Lifecycle at Microsoft



Sample of TwC Output So Far:

- Microsoft Products
  - Windows Defender - antispyware tool
  - Microsoft Windows XP Service Pack 2. – safeguard from hackers, viruses, etc.
  - Fighting spam and filtering content. – 3+ billion spam e-mails are blocked daily
  - Microsoft Phishing Filter - anti-phishing add-in in Hotmail and I.E 7.0
  - Rights Management. - protect content at the file level regardless of where it goes.
  - MSN. - Parental Controls, Pop-Up Guard, Junk E-mail Guard
  - Sender ID. - Collaboration with industry to stop domain Spoofing
  - Privacy tools for removing unwanted software.
- Global Privacy Processes
- Customer Education & Resources (Be Web Aware)
- Thought Leadership – Identify Management

"Four years ago, Microsoft committed to Trustworthy Computing. Today, that commitment is even stronger—it's part of our daily corporate culture."

Trustworthy Computing VP Scott Charney

New Technology Enhancements

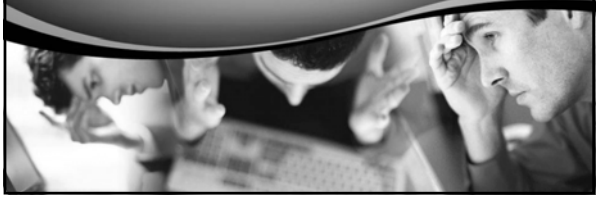
- Windows Rights Management
- Windows Vista
- Internet Explorer 7
- Office 2007
- Exchange 2007
- SharePoint / Groove
- Audit Collection Services

Microsoft's Security Vision Is Much More...

Establishing **trust** in computing to realize the full potential of an interconnected world

The Internet Identity Crisis

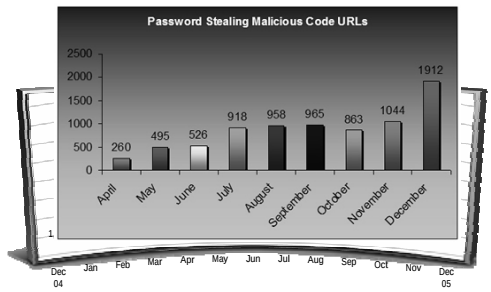
- Phishing & Phraud
- Password fatigue
- Inconsistent, proprietary identification mechanisms



Password Fatigue

Have we been conditioned to be phished?

Phishing & Phraud



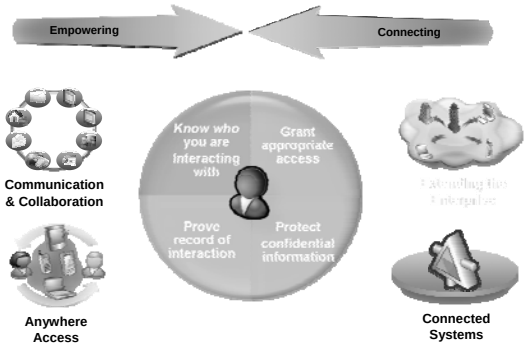
Source: http://www.antiphishing.org

Identity Facts

- Too Many User Repositories
  - Enterprises have 68 internal and 12 external account directories
  - 75% of internal users and 38% of external users are in multiple stores
- Increasing IT Operational costs
  - 45% of all help desk calls are for p/w resets
  - Organizations are managing on average 46 suppliers, spending over 1380 hours managing changes to access privilege.
- Inefficient Account Provisioning/De-Provisioning
  - User management consumes 34% of the total time IT spends on IdM
  - User accounts get created in 16 systems and deleted in 10.
- Impact on User Productivity
  - On average IT is managing access to 73 unique applications requiring user access.
  - Average user spends 16 minutes a day for logins
  - SSO increases user productivity by 15% and efficiency by 18%

Source: META Group research conducted on behalf of PricewaterhouseCoopers, June 2002, MSFT Internal

The Power of Identity



What is Identity Management?

Directory Services	Repositories for storing and managing accounts, identity information, and security credentials.
Access Management	The process of authenticating credentials and controlling access to networked resources based on trust and identity.
Identity Lifecycle Management	The processes used to create and delete accounts, manage account and entitlement changes, and track policy compliance.

What is a digital identity?

- A set of **claims** someone makes about me
- Claims are packaged as security tokens
- Many identities for many uses
- Useful to distinguish from **profiles**

Identity is Matched to Context

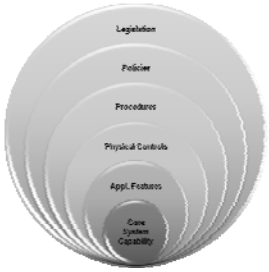
In Context
- Bank card at ATM
- Gov't ID at border check
- Coffee card at coffee stand
- MSN Passport at HotMail

Out of Context
- Coffee card at border check

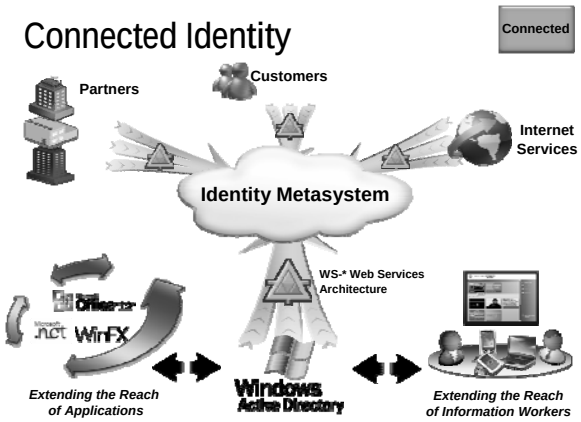
Maybe Out of Context?
- Gov't ID at ATM
- SSN as Student ID
- MSN Passport at eBay

IDM requires a layered approach

- Multidisciplinary approach is required to address:
  - Business, policy, people and technology aspects of ID
- Allows for the allocation of controls outside of IT



Connected Identity



Overview of Health Policy as it Pertains to Electronic Personal Health Information

Ross Hodgins, Director of Access and Privacy Division, Health Canada

Abstract:
Improved information technology provides easier access to information, yet it can increase the risk of privacy breaches. This presentation will review key federal privacy legislations and policies (including the Privacy Act, Access to Information Act, Pan-Canadian Privacy and Confidentiality Framework and PIPEDA) that pertain to personal health information in general and electronic health information specifically. Policy and awareness raising initiatives currently in place at Health Canada in implementing these legislations and policies will be highlighted.

Bio:
Ross Hodgins is Director/Coordinator of the Access to Information and Privacy Division in Health Canada. He is responsible for establishing a centre of expertise within the Department and for collaborating with representatives from the health sector to advance the protection of privacy and mitigate privacy risks. In addition, he manages the operational unit that responds to access to information and privacy requests.

Prior to working at Health Canada, Ross was a Senior Privacy Advisor at the Treasury Board Secretariat. During his career at the Secretariat he developed several information management, communication, access to information and privacy policies. In the privacy field, he implemented government-wide policies and guidelines related to data matching, control of the Social Insurance Number and privacy impact assessments. He also established the Info Source program which is a series of publicly-available databases and publications describing the Government of Canada, its programs, services and information holdings.

Ross has a Masters of Library and Information Sciences from the University of Western Ontario.

Health Canada Santé Canada

Overview of Health Policy as it Pertains to Electronic Health Information

Electronic Health Information & Privacy Conference
November 13, 2006

Ross Hodgins
Director / Coordinator
Access to Information and Privacy Division

Canada

Health Canada Santé Canada

Legislative Framework

- 23 privacy acts throughout Canada
- Federal
  - *Privacy Act*
  - *Personal Information Protection and Electronic Documents Act (PIPEDA)*
- Provincial / Territorial
  - *Freedom of Information and Privacy Acts*
  - Private sector privacy acts
  - Health information acts

Canada

2

Health Canada Santé Canada

Challenges

- To respond to Canadians' privacy and confidentiality expectations
- To harmonize federal/provincial/territorial privacy regimes
- To provide practical policies and guidelines that reflect the realities and requirements of the health system
- To ensure a consistent approach in the development and deployment of pan-Canadian electronic health records solutions

Canada

3

Health Canada Santé Canada

Electronic Health Records

- Pan-Canadian electronic health record system is a priority of Ministers of Health and Deputy Ministers of Health
- Critical to improving patient safety and the quality of health care services for Canadians
- Recognized as an innovative vehicle to improve and sustain Canada's health care system
- Federal/provincial/territorial partnership with Canada Health Infoway

4

Health Canada Santé Canada

Electronic Prescribing

- Key element of the electronic health record
- Refers to the transfer of information about prescriptions from practitioner to the pharmacist
- Under the *Food and Drug Regulations* and the *Narcotic Control Regulations*, prescriptions can only be communicated in written format or verbally
- *PIPEDA, Part II* allows for the electronic transfer of documents when legislation requires them to be in writing, provided certain conditions are met
- Canada Health Infoway developing standards
- Health Canada adjusting regulations

5

Health Canada Santé Canada

Pan-Canadian Health Information Privacy and Confidentiality Framework

- Set of harmonized principles and provisions for the collection, use, disclosure and protection of personal health information
- Conference of F/P/T Deputy Ministers recognized that the *Framework* will serve as a basis to
  - review and revise, as necessary, existing legislation, or
  - enact new legislation in each jurisdiction reflecting the rules in the agreed-to *Framework*

6

Health Canada Santé Canada

PIPEDA Awareness Raising Tools (PARTs)

- Series of communication tools designed to assist the health care sector to understand the scope and requirements of *PIPEDA*
- 75 questions and answers, e.g. What additional responsibilities will be added to health professionals as a result of *PIPEDA*?
- Glossary of terms, e.g. circle of care
- Sample brochure and poster
- Available on the web sites of Health Canada, Industry Canada and the federal Office of the Privacy Commissioner

7

Health Canada Santé Canada

Selected Privacy Issues

- Definitions of personal information and personal health information
- Consent for collection, use and disclosure of personal information for health care
- Use and disclosure of personal information without consent for research
- Disclosure of personal information without consent for surveillance
- Disclosure of personal information without consent in the public interest
- Outsourcing and transborder flows of personal information

8

Health Canada Santé Canada

Definitions of Personal Information and Personal Health Information

- Information about an identifiable individual
- Recorded and unrecorded information
- Business contact information

9

Health Canada Santé Canada

Consent for Collection, Use and Disclosure of Personal Information for Health Care

- Consent rules vary substantially under Canadian privacy legislation
- Public sector privacy legislation allows for collection of personal information without consent for the purposes of operating a program and permits use and disclosure for "consistent uses"
- *Pan-Canadian Health Information Privacy and Confidentiality Framework* recognizes
  - privacy as a consent-based right
  - implied, knowledgeable consent within the circle of care
  - express consent for disclosures of personal information outside the circle of care

Canada

10

Health Canada Santé Canada

Use and Disclosure of Personal Information Without Consent for Research

- General privacy legislation permits use and disclosure of personal information for research without consent but with varying levels of conditions
- Health sector privacy legislation permits use and disclosure of personal information provided notice is given of the intended research and there is reference to applicable privacy regulatory authorities

Canada

11

Health Canada Santé Canada

Disclosure of Personal Information Without Consent for Health Surveillance

- All privacy statutes allow for disclosure of personal information without consent where required by law and in emergency circumstances
- Health sector privacy legislation permits disclosure of personal information without consent subject to certain constraints
- Requirement for health protection legislation to balance authorities to collect, use and disclose personal information with appropriate checks

Canada

12

Health Canada Santé Canada

Use and Disclosure of Personal Information Without Consent in the Public Interest

- Public sector privacy statutes allow for disclosure of personal information without consent in the public interest with reference to oversight bodies
- Health sector privacy legislation does not contain an explicit public interest exception but allows for disclosures of personal information without consent in extraordinary circumstances

13

Health Canada Santé Canada

Outsourcing and Transborder Flows of Personal Information

- Privacy legislation treats transborder data flows inconsistently, e.g.
  - no reference
  - permitted to provide health care to individuals
  - permitted with safeguards, such as written agreements
  - custodians required to take reasonable steps to protect the information
- Outsourcing of program administrative functions continues to be a significant concern

14

Health Canada Santé Canada

Organizational Challenges

- Compliance
  - Need to ensure compliance with legislation, policies and guidelines
- Mitigation of privacy risks
  - Privacy requires a shared management approach
  - Corporate, branch, and regional privacy activities must fit within a coherent organizational approach
  - Privacy expertise and support need to be available to all staff

15

Health Canada Santé Canada

Organizational Initiatives

- Legislative renewal
- Corporate policy and guidelines
- Data sharing
- De-identification / re-identification
- Research Ethic Boards
- Privacy Impact Assessments
- Training and awareness
- Education

16

Health Canada Santé Canada

Legislative Renewal in Health Canada

- Modernize older health protection statutes under a comprehensive framework
- Determine the right balance between
  - the need for Health Canada to have access to information for public health purposes and
  - the need to protect the privacy and confidentiality of sensitive personal and commercial information, particulary in electronic environments
- Resolve regulatory gaps hampering technological uses, e.g. e-prescribing
- Ensure that the renewal proposals are aligned with the *Pan-Canadian Health Information Privacy and Confidentiality Framework*

17

Health Canada Santé Canada

Corporate Privacy Policy

- To improve privacy management
- To promote greater compliance with privacy
- To respond to the needs of staff
- To demonstrate due diligence
- To foster and facilitate horizontal management of privacy by means of training and awareness

18

Health Canada Santé Canada

Data Sharing

- To develop policies and guidelines to meet privacy obligations when sharing personal information
- To provide practical tools for program managers to ensure privacy is addressed in all data sharing arrangements
- To ensure that related issues, such as de-identification/re-identification, are taken into account

19

Health Canada Santé Canada

De-identification / Re-identification

- Policy to provide a set of principles that
  - balance the need for openness and transparency and the need to protect personal information
  - support an accountability structure
- Guidelines and best practices to assist program managers in
  - the development and maintenance of databases that support program objectives and address the risks of re-identifying individuals pursuant to disclosure of data
  - de-identifying data sets for uses beyond the original purpose

20

Health Canada Santé Canada

Research Ethics Boards

- To build on existing guidelines and develop best practices to assist researchers in addressing privacy issues when preparing proposals for REBs
- To partner with national research ethics organizations to develop tools to assist members of REBs in evaluating proposals involving the collection, use and disclosure of personal information
- To develop training and awareness tools specifically for researchers and members of REBs

21

Health Canada Santé Canada

Privacy Impact Assessments

- Government-wide / cross-jurisdictional
  - Policies and guidelines
  - Courses for managers / practitioners
  - Audit guides
- Organizational
  - Fact sheets
  - Toolkit
  - Training and awareness
  - Standing offers

22

Health Canada Santé Canada

Training and Awareness

- Privacy courses - Basics / Advanced
- Targeted privacy courses – Researchers / Surveillance
- Privacy Impact Assessment courses - Basics / Advanced
- Information Management – Orientation presentations and videos
- Electronic learning tools

23

Health Canada Santé Canada

Education

- University of Alberta certificate course on privacy and personal health information
- Collaboration between
  - University of Alberta
  - Office of the Information and Privacy Commissioner of Alberta
  - Office of the Privacy Commissioner of Canada
  - Health Canada
- Course to be launched in September 2006 in both official languages

24

Health Canada Santé Canada

Federal/Provincial/Territorial Health Privacy Network

- Establish a pan-Canadian network of health privacy contacts
- Identify emerging privacy issues of mutual concern
- Provide consistent advice
- Share existing privacy tools
- Develop generic policies and guidelines in relation to personal health information

25

Health Canada Santé Canada

Thank You!

Ross Hodgins
Director / Coordinator
Access to Information and Privacy Division
Health Canada
613-946-3179
ross_hodgins@hc-sc.gc.ca

26

Health Chips? Using Implantable RFID to link Patients to Health Records
Ian Kerr, University of Ottawa

Abstract:
Since the US Food and Drug Administration approved VeriChip as a medical device in October, 2004, 232 doctors in 80 hospitals have elected to use the implantable VeriMed Patient Identification system as a means of linking patients to electronic health care records. Although Canada's Therapeutic Products Directorate has not yet approved the implantable RFID technology for use in Canada, the VeriChip corporation has recently opened offices in Vancouver and Ottawa. This presentation examines some of the legal and ethical issues of the VeriMed Patient Identification system in and out of the hospital setting.

Bio:
Prior to his appointment to the Faculty of Law at the University of Ottawa in 2000, Ian Kerr held a joint appointment in the Faculty of Law, the Faculty of Information & Media Studies and the Department of Philosophy at the University of Western Ontario. His devotion to teaching has earned six awards and citations, including the Bank of Nova Scotia Award of Excellence in Undergraduate Teaching, the University of Western Ontario's Faculty of Graduate Studies' Award of Teaching Excellence, and the University of Ottawa's AEECLSS Teaching Excellence Award. Professor Kerr currently teaches a graduate seminar in the LLM concentration in law and technology (Technoprudence: Legal Theory in an Information Age), as well as a unique seminar offered each year during the month of January in Puerto Rico that brings students from very different legal traditions together to exchange culture, values, and ideas and to unite in the study of technology law issues of global importance (TechnoRico). Professor Kerr also teaches in the areas of moral philosophy and applied ethics, internet and ecommerce law, contract law and legal theory.

In 2001, Professor Kerr was awarded the Canada Research Chair in Ethics, Law and Technology. He has published writings in academic books and journals on ethical and legal aspects of digital copyright, automated electronic commerce, artificial intelligence, cybercrime, nanotechnology, internet regulation, ISP and intermediary liability, online defamation, pre-natal injuries and unwanted pregnancies. His current program of research includes two large projects: (i) On the Identity Trail, supported by one of the largest ever grants from the Social Sciences and Humanities Research Council, focusing on the impact of information and authentication technologies on our identity and our right to be anonymous; and (ii) An Examination of Digital Copyright, supported by a large private sector grant from Bell Canada and the Ontario Research Network in Electronic Commerce, focusing on various aspects of the current effort to reform Canadian copyright legislation, including the implications of such reform on fundamental Canadian values including privacy and freedom of expression.

Dr. Kerr is a member of the Law Society of Upper Canada, the Academic Coordinating Committee of the Centre for Innovation Law and Policy, the Centre for Ethics and Values, the Canadian Association of Law Teachers, the Canadian Bar Association, and the Uniform Law Commission of Canada's Special Working Group on Electronic Commerce. He is an associate editor of Kluwer's Electronic Commerce Research Journal, a guest editor for Presence: Teleoperators and Virtual Environments (MIT Press), and sits as a member on the Advisory Board of the Canadian Internet Policy and Public Interest Clinic and on the Advisory Board of Butterworths' Canadian Internet and E-Commerce Law Newsletter. He is also co-author of Managing the Law (Prentice Hall), a business law text used by thousands of students each year at universities across Canada.

health chips?

using implantable rfid to link patients to health records

 iankerr
canada research chair in ethics, law & technology
university of ottawa

rfid

(ar-fids)

I. rfid 101
II. villa olympica
III. verimed™ patient identification
IV. personal area networks
V. regulating (implantable) rfid
VI. policy discussion


jereMe

shout out


angela


jason

rfid 101

three years ago…

anonequity.org

walmart / DoD

anonequity.org

supply chain

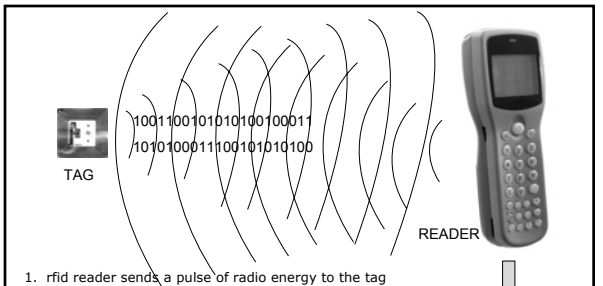
anonequity.org

internet of things

anonequity.org

(ubiqcomp)

anonequity.org



anonequity.org

anonequity.org

novel characteristics

- unique identifier
- extended range
- increased penetration
- read /write
- kill switch

anonequity.org

legal issues

- consumer tracking
- deactivation at point of sale (?)
- labeling law
- consumer choice (?)
- fipps

anonequity.org

oipc guidelines

Focus on RFID information systems, not technologies:
> privacy implications not inherent but based on deployment
> policy must be systemic rather than focused on any given technology

Build in privacy and security from the outset – at the design stage:
> technological solutions must also be systemic
> RFID systems should address the privacy/security issues at the design stages
> emphasis on minimizing: identifiability, observability and linkability

Maximize individual participation and consent:
> Use of RFID systems should be as open and transparent as possible
> RFID systems should afford individuals with opportunity to make informed decisions.

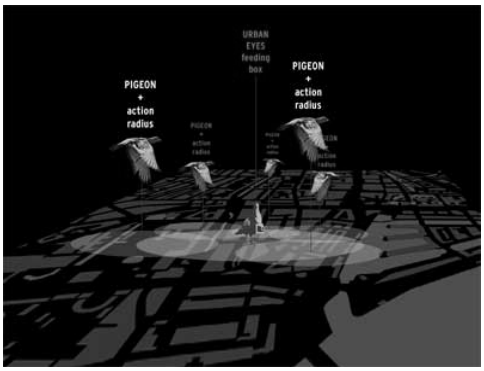
anonequity.org

anonequity.org

anonequity.org

anonequity.org

anonequity.org



anonequity.org

cctv london

anonequity.org

villa olympica

anonequity.org

anonequity.org

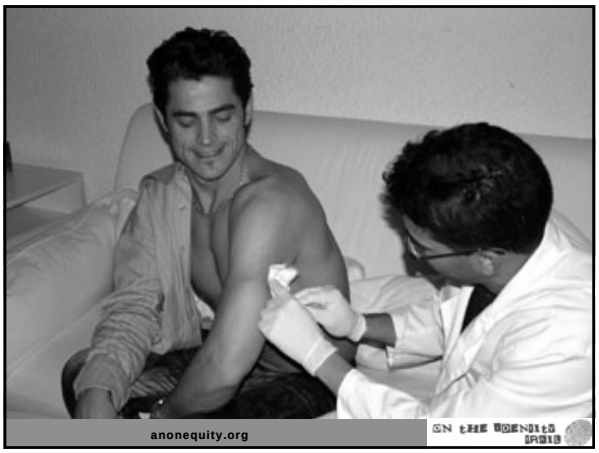
conrad's biz plan

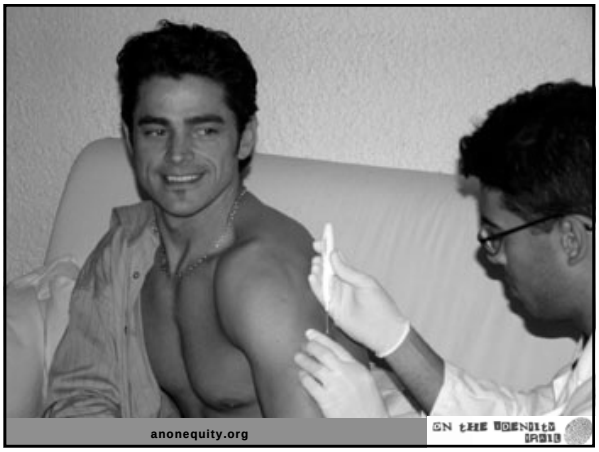
anonequity.org

VIPchip

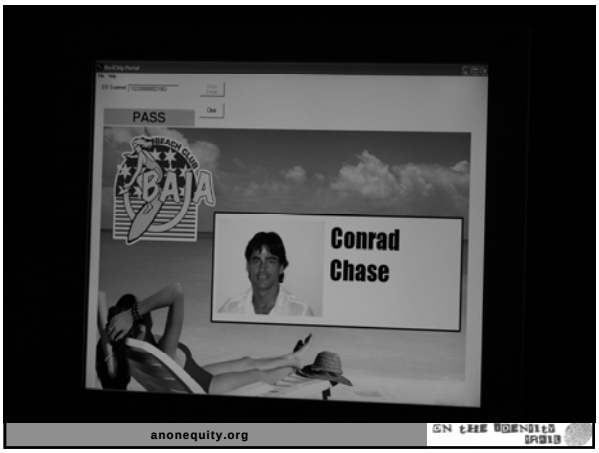
anonequity.org

anonequity.org





verichip reader



anonequity.org

ON THE UNITED IRIS

"the objective of the technology is to bring an ID system to a global level that would destroy the need to carry ID documents and credit cards."

conradchase

anonequity.org

ON THE UNITED IRIS

jumping on the implantable chipwagon…

anonequity.org

ON THE UNITED IRIS

headline news

anonequity.org

ON THE UNITED IRON

Digital Angel

anonequity.org

ON THE UNITED IRON

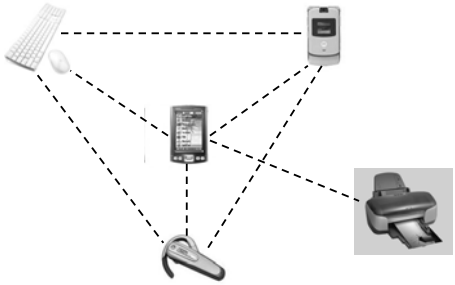
Digital Angel

anonequity.org

ON THE UNITED IRON

wifi

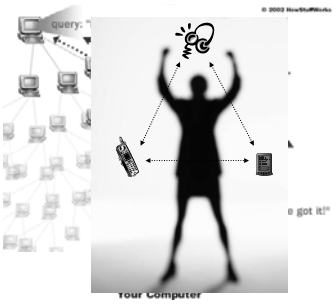
(ad hoc sensor networks)



anonequity.org

from LANs to PANs

LANs
(local area networks)
↓
WANs
(wide area networks)
↓
PANs
(personal area networks)



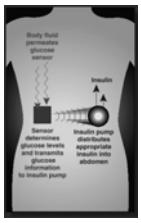
anonequity.org

kevinwarwick

- kevin warwick wants to make PANs really personal
- neural transducer implant
- surgical implant allows recording and transmission
- allows reception of signals

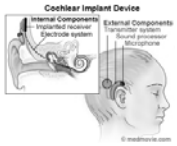
anonequity.org

implantable devices (i)



- insulin pumps and sensor systems
- insulin is delivered on demand
- wireless link between pump, sensor, and controller

implantable devices (ii)



- cochlear implants
- phones, MP3 players, etc. can be linked
- wireless communication
- current research includes a bluetooth cell phone link

adding implantable devices to the PAN

nature of the info exchange

from

- contact lists
- emails
- credit card info

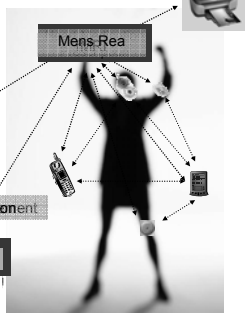
to include

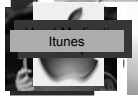
- real-time physiology (blood sugar/type/alcohol)
- sights and sounds
- neural signals (sensations, feelings, thoughts?)

security and privacy needs are heightened

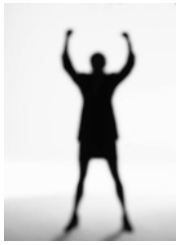
data flow in/out of the PAN

- PAN routers will most likely be used to optimize data flow within the PAN
- Vendors will want to push data to PANs in exchange for $ or services
- Other service providers will want to push/pull data from the PAN





netvolution



the network of ideas

↓

the network of things

↓

the network of people

"we are considering not merely a physical extension of human capabilities but rather a completely different basis on which the [nervous system] operates in a mixed human, machine fashion."

kevinwarwick

"a human whose nervous system is linked to a computer not only puts forward their individuality for serious questioning but also, when the computer is part of a network or at least connected to a network, allows their autonomy to be compromised."

kevinwarwick

ipv6

health ↔ info tech

anonequity.org

verimed™

anonequity.org

regulation in canada

- *s. 30(a)(iii) food and drugs act*
  - *medical devices regulations*
    - to ensure that all medical devices offered for sale in Canada meet basic safety and efficacy requirements
- no device that falls within the definition of a "medical device" under the act can be sold in canada without the approval of the tpd and a corresponding license.

anonequity.org

what is a 'medical device?'

"device" means any article, instrument, apparatus or contrivance, including any component, part or accessory thereof, manufactured, sold or represented for use in:

(a) the diagnosis, treatment, mitigation or prevention of a disease, disorder or abnormal physical state, or its symptoms, in human beings or animals,

(b) restoring, correcting or modifying a body function or the body structure of human beings or animals,

(c) the diagnosis of pregnancy in human beings or animals, or

(d) the care of human beings or animals during pregnancy and at and after birth of the offspring, including the care of the offspring, and includes a contraceptive device but does not include a drug

verichip ≠ medical device

verichip ≠ ehr !

VeriChip = uniqueID + 

anonequity.org

read--only

anonequity.org

unencrypted

anonequity.org

cloning verichip

anonequity.org

BIObonding

anonequity.org

anonequity.org

Q: appropriate regulatory policy?

broader ethical Qs

- is there a moral distinction between wearing and implanting RFID?
- are there moral limits to the integration of humans and machines?
- how should scientists/technologists/law makers deal with the problem of "reductionism"?

health policy Qs

- *hospital policy*
  - should hospitals in Canada adopt a voluntary verichip program?
  - under what circumstances/conditions?
- *regulations*
  - what are the pros/cons of regulating verichip as a medical device?
  - who should be permitted to implant chips?
- *legislative reform*
  - is new legislation/regulations necessary to deal with hybrid IT/health issues arising from the human-machine merger

ON THE IDENTITY TRAIL

anonequity.org

idtrail.org

anonequity.org

blog*on*nymity

anonequity.org

iankerr@uottawa.ca

anonequity.org

Legal Challenges Surrounding Electronic Health Record Systems
Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada

Abstract:
Pan-Canadian, interoperable electronic health record (EHR) systems present exciting promise and opportunity for payers, managers, providers, researchers and users of the health system. The development of such systems, however, comes with a host of related challenges, not least of which is the protection of personal health information. This presentation will examine some of the privacy challenges raised by:

- jurisdictional issues in the context of interoperable systems involving trans-border data-flows;
- accountability and stewardship responsibilities among various players in the system;
- secondary use of EHR data for health research purposes, as well as other purposes including insurance and employment; and,
- real-life implementation issues that require practical compliance measures for even the best legal rules to work.

The presentation will go on to discuss the various efforts being made by the Office of the Privacy Commissioner of Canada to fund critical research in this area, to partner with provinces in assessing and building necessary capacity for effective privacy oversight, and to work collaboratively with key stakeholders, including Canada Health Infoway Inc.

Bio:
Patricia is the General Counsel of the Office of the Privacy Commissioner of Canada (OPCC), and is responsible for: directing the provision of legal advice on a broad range of policy and legislative initiatives; representing the OPCC before Parliamentary Committees and other relevant venues; overseeing the preparation and conduct of litigation; directing research and development of innovative legal approaches to deal with new and complex privacy issues; working collaboratively with stakeholders across jurisdictions, in both public and private sectors.

Prior to joining the OPCC, Patricia spent five years (Jan. 2000 – Jan. 2005) building and heading up the Ethics Office of the Canadian Institutes of Health Research, mandated to: 1) lead and respond to the development of health policy from an ethical, legal and social perspective; 2) promote a robust culture of ethics and integrity in health research; 3) strengthen Canada's research capacity to develop, integrate and apply new knowledge in ethics, law and social sciences to the health sector.

In the spring of 2002, Patricia was temporarily seconded for a few months to Canada Health Infoway Inc. to contribute her legal and privacy expertise to a team of expert consultants advising on the development of the company's inaugural business plan.
For over six years (1992-93, 1994-1999), Patricia practiced in Montreal with a major national law firm (Heenan Blaikie), researching, litigating and advising clients in the areas of health law, human rights, labour and employment law, civil litigation and professional regulation/liability.

Patricia has served on the Board of Directors of non-profit community organizations, and has participated as volunteer member of a hospital research ethics board, clinical ethics committee, and several governmental advisory committees. She has published numerous papers and presented at multiple conferences and meetings across the country on topics related to health law, privacy and ethics.

Patricia is a member of the Quebec and Canadian Bar Associations since 1993. She obtained degrees in business (1987), common law (1992) and civil law (1992) from McGill University, as well as a Masters Degree in Medical Law and Ethics (1994) from King's College in London, U.K.

Office of the Privacy Commissioner of Canada

Electronic Health Information & Privacy Conference

Ottawa, Ontario

November 13, 2006

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Legal & Practical Challenges of Protecting Privacy in an EHR World

Patricia Kosseim
General Counsel
Office of the Privacy Commissioner of Canada
pkosseim@privcom.gc.ca

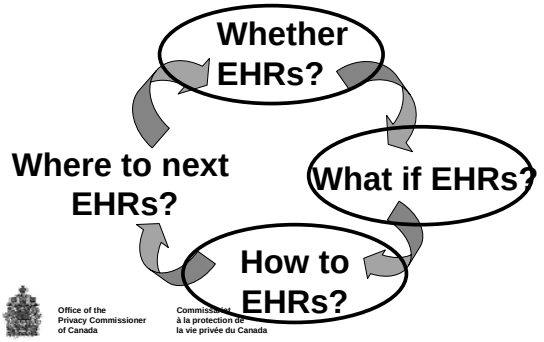
Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Evolutionary Debate

- **Whether EHRs?**
- **What if EHRs?**
- **How to EHRs?**
- **Where to next?**

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Iterative & Ongoing Debate



Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Outline

- Legal & Practical challenges
  - Jurisdictional issues
  - Accountability & stewardship
  - Secondary uses
  - Practical implementation
- Research done or underway
- Stakeholder Collaborations

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Jurisdictional Issues

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Accountability & Stewardship

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Secondary Uses

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Practical Implementation

"In theory, there is no difference between theory and practice. But, in practice, there is."
-- Jan L.A. van de Snepscheut

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

OPC-Funded Research

- **Centre de Bioéthique, IRCM**
  (re:Secondary Uses of EHRs)
- **Memorial University, Nfld.**
  (re: Technology Choices & Privacy Policy)
- **CHEO Research Institute, Ottawa**
  (re: Pan-Canadian De-identification Guidelines for PHI)
- **University of Alberta**
  (re: EHRs and PIPEDA)

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Capacity-building

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Stakeholder Collaborations

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Conclusion

"Supposing, Pooh", said Piglet, "we were walking in the forest and a tree fell on us."

"Supposing it didn't", said Pooh after careful consideration.

A.A.Milne (1882-1956), British writer and Poet.

The House at Pooh Corner (1928)

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

pkosseim@privcom.gc.ca
www.privcom.gc.ca

THANK YOU / MERCI!!

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Consumer Information as Commodity: The Databrokerage Industry & its Implications for Health Privacy

Philippa Lawson, Executive Director – Canadian Internet Policy & Public Interest Clinic (CIPPIC)

Abstract:
There is a large and vibrant trade in the personal information of Canadian consumers, both within Canada and more widely in North America. This trade is driven by the direct marketing industry and competition among retailers and fundraisers for customers and donors. Some consumer information is health-related, and can be used to develop profiles based on personal health status or concerns of individuals. Such profiles are extremely valuable to those marketing health products and services. However, they necessarily involve the collection and disclosure of sensitive information about individuals (accurate or inaccurate), thus raising serious privacy concerns. Is this trade adequately regulated from a privacy perspective? How are marketers complying with data protection laws? This presentation will review the findings of a recent study of the Canadian databrokerage industry and consider its implications for health privacy.

Bio:
Before joining the University of Ottawa as Executive Director of the newly formed Canadian Internet Policy and Public Interest Clinic (CIPPIC) in 2003, Pippa Lawson was senior counsel at the Public Interest Advocacy Centre (PIAC), where she practiced consumer advocacy and administrative law for twelve years. PIAC is an Ottawa-based organization that represents the interests of under-represented individuals and groups on issues of broad public concern. Pippa has a Master's degree from the Norman Paterson School of International Affairs (1986) and a Law degree from Queen's University (1989). At PIAC, Pippa led consumer interventions in all major telecommunications proceedings before the Canadian regulator since 1991. She also acted for consumer groups in regulatory matters before the Ontario Energy Board, and represented various public interest parties before the Federal and Supreme Courts of Canada on matters ranging from the abandonment of railway lines to voting rights. At CIPPIC, Pippa has focused on issues involving new technologies and copyright, privacy and consumer protection law. Her areas of expertise are telecommunications regulation, privacy and consumer protection in electronic commerce.

As a representative of the consumer interest on privacy issues before policy and law-making bodies, Pippa is highly qualified to identify and assess privacy issues arising from new technologies, laws and business practices.

Consumer Health Information as Commodity

Presentation to the
Electronic Health Information and Privacy Conference
Ottawa, November 13, 2006

Philippa Lawson
Executive Director & General Counsel, CIPPIC
University of Ottawa, Faculty of Law
www.cippic.ca

CIPPIC Data broker study

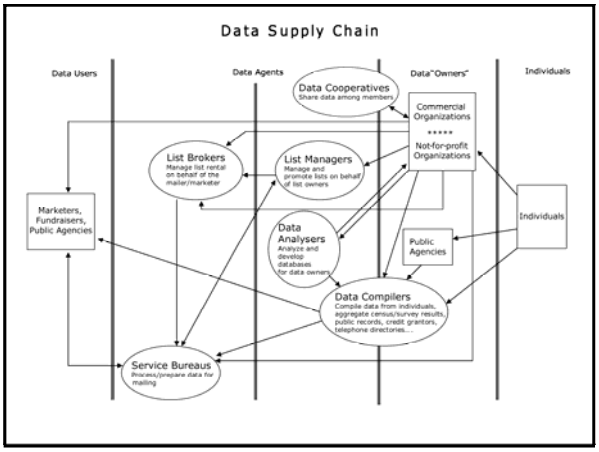
- 2005-2006; funded by OPCC & SSHRC
- Purpose:
  - to understand and describe how detailed personal information about Canadians gets into the hands of organizations with whom they have no relationship

Data broker study

- Scope:
  - Canadian market
  - consumer information
  - trade (vs. internal use)
  - bulk (vs. individual searches)
  - no exam of spyware or related tools
  - limited research on end-uses
  - no privacy assessments

Data broker study

- Methodology:
  - consultation with industry experts
  - ATIP requests
  - online searches
  - trade journal/email bulletin subscriptions
  - direct marketing websites/portals
    - review of datacards
    - follow-up with list managers/data compilers



Consumer Lists

- Consumer names and addresses by (eg):
  - subscription to particular magazine
  - type of book purchases
  - online registrations to certain sites
  - responders to direct mail/TV/radio/internet solicitations
  - responders to “money-making opportunities”
  - holders of particular credit/reward cards
  - type of investments owned/plan to buy
  - automobile, electronic products owned/plan to buy
  - frequent air travellers
  - beach resort goers
  - pet ownership
  - causes to which they donate

Consumer Lists

- focus on:
  - hobbies and interests
    - inferred from purchases/subscriptions, or as expressed in surveys
  - opportunity seekers; “suckers”
    - inferred from responses to advertisements
  - high spenders
    - inferred from purchase info., e.g., auto, electronics
  - health/dietary concerns
    - inferred from purchases/subscriptions or as expressed in surveys

List enhancements

- geographic area
- demographics:
  - gender, age,
  - marital status, family size, children’s ages
  - race, ethnicity
  - religion
  - occupation
  - level of education
  - type of housing/home ownership
  - household income
- mail order buyers
- presence of credit card
- interests & lifestyles

Group Profiles

- Geo-demographic/psychographic profiles

  Eg: “Cosmopolitan Elite”, “Elder Harbour”, “Lunch at Tim’s”, “Bicycles and Bookbags”, “Jeunes et Actifs”, “Young Technocrats”, “Quebec Rural Blues”, “Electric Avenues”…

- Credit profiles - by postal code or other small geographic area

Data Sources

- Subscriptions
- Purchases: mail order, online, etc.
- Contest entries
- Rebates
- Special offers
- Sign-up programs
- Online registrations
- Online activity (clickstream data)
- Product warranty/registration cards
- Surveys

Sources: Surveys

- Retailer-specific surveys
  - diagnostic (websites), customer satisfaction, special offers….
- Survey-based data brokers
  - ICOM
    - >2 m. Canadian households (>1m/year)
  - Bluelist.ca
    - >1 m. surveys returned each year
  - BBM (> 50,000), PMB (>24,000)
    - aggregated info only (for broadcasters and print media advertisers)
- Stats Can Census
  - aggregated only (to 40 households min)

Consumer Lists – health related

- Alternative Medicine Literature Buyers
- Health and Fitness Magazine Subscribers
- Herbal Medicine Users
- Medical Literature Buyers
- Natural Medicine Courses Attendees
- Stress Management Courses Attendees
- Up-Market Fitness Club Members
- Weight Loss Program Buyers

Specific Lists - Cdn

- IMMUTOL Mail Order Buyers - Canada
- Canadians with hearing aids
- Alterna Holistic Health Buyers – Cdn
- Bio-mince Canadian Diet
- French Canadian Weight Loss Subscribers
- Expecting a baby
- Nutrition and Diet
- Canadian Healthy Living Aspirants
- Preval Health Products – Canadian

Preval Health Products

"These health conscious buyers have purchased primarily skin zinc (skin therapy) and actifade (age spot reversal) as well as other health/beauty products from radio spots and space ads. They have spent an average of $45.00 (u.S. Dollars) and most have paid by bank credit card."

IMMUTOL® Mail Order Buyers

Canada Counts: 21,641

This mailing list is an audience of individuals who are interested in preventing the consequences of a weak immune system, which can include cancer, viral syndromes, (chronic fatigue, Epstein Barr, herpes, HIV), parasitic and bacterial infections, or any other immune problems such as colds, flu, and allergies. They have purchased IMMUTOL® , which has been clinically tested, and recommended by physicians for strengthening the immune system. All these individuals have paid $59.95 for the first month's supply, and $41.97 for subsequent months.

Target this audience with offers for health/vitamins, anti-aging, potency, insurance, travel, insurance, and more.

Alterna Holistic Health Buyers

"The buyers here spend an average of $150.00 per month on products such as magnetic health therapy devices, massage products, aloe products, chemical free health and home products, vitamins and herbal supplements.

Age, income, product and lifestyle selects are available."

Lombardi's Health Masterfile

"...comprised of Lombardi's Doctors Health Press newsletter subscribers. The majority of the file is comprised from subscribers to: Doctors Journal of Alternative Remedies, Doctors Natural Cures, The Vitamin Doctor, The Healing Doctor, The Food Doctor, The Weight Loss Doctor, Cures to Hidden Illnesses, Homeopathic Healing and the Chinese Medicine newsletters.

These subscribers have an interest in health and wellness, weight loss, alternative medicines, vitamins and supplements, fitness and pain relief."

Canadian Health Newsletter Masterfile

- subscribers of health-related newsletters: Heart Advisor, Women's Health Advisor, Focus on Healthy Aging, Food and Fitness Advisor, Men's Health Advisor, HealthNews and Arthritis Advisor.
- "Reach direct mail responsive, health-conscious men and women with an average age of 50 and an average HHI of $55k. These subscribers are ideal prospects for fundraising, health & fitness, supplements, catalog, self improvement, travel and book offers."

Health Care Professionals

"The Health Care Professionals here are all at home address and are listed by specialty and interest."

ICOM Targetsource

"ICOM's TargetSource Health Database:

- *is the largest permission-based health database in North America (with 1.1 million new Canadian responders per year), providing you with a larger audience of new consumers/patients.*
- *is single-sourced from accurate survey data, giving you better results from direct mail responsive consumers*
- *provides you with multiple cost-effective communication options, including e-mail, to maximize your ROI"*

ICOM Health Database

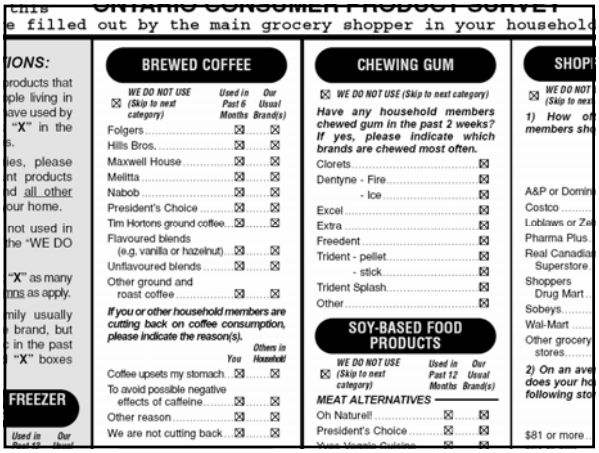
- Family health (40 diseases/problems)
- Medications:
  - Allergies or Sinus
  - Adult Pain Relievers
  - Arthritis Pain Relief
  - Children's Cold Remedies
  - Heartburn Remedies
  - Diarrhea Medications
  - Yeast Infection Medications
  - Psoriasis
  - Prescription Meds: Imitrex, Lipitor, Viagra
- "Volumetrics"
- Nutrition and Diet

ICOM – Health Database

"Call us about participating in ICOM's Shopper's Voice™ Survey and gather custom data specific to your business needs from up to 1.1 million direct mail responsive consumers per year. ICOM will work with you to develop a custom question that will identify your most valuable health care consumers."

ICOM – Data Source

"The opt-in question on our Shopper's Voice survey provides consumers the opportunity to specify their willingness to receive or deny further postal or e-mail offers. Any consumer list coming from ICOM includes the responder's consent to receive further offers so mailers are assured that consumer privacy is being respected."



e filled out by the main grocery shopper in your household

BREWED COFFEE

☒ WE DO NOT USE (Skip to next category)	Used in Past 6 Months	Our Usual Brand(s)
Folgers	☒	☒
Hills Bros.	☒	☒
Maxwell House	☒	☒
Melitta	☒	☒
Nabob	☒	☒
President's Choice	☒	☒
Tim Hortons ground coffee	☒	☒
Flavoured blends (e.g. vanilla or hazelnut)	☒	☒
Unflavoured blends	☒	☒
Other ground and roast coffee	☒	☒

If you or other household members are cutting back on coffee consumption, please indicate the reason(s).

	You	Others in Household
Coffee upsets my stomach	☒	☒
To avoid possible negative effects of caffeine	☒	☒
Other reason	☒	☒
We are not cutting back	☒	☒

CHEWING GUM

☒ WE DO NOT USE (Skip to next category)

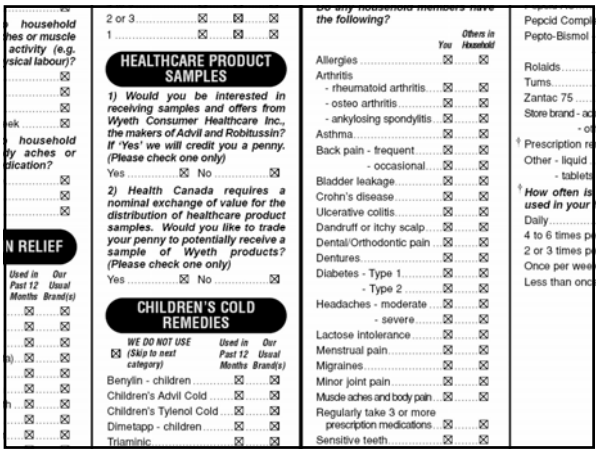
Have any household members chewed gum in the past 2 weeks? If yes, please indicate which brands are chewed most often.

Clorets ☒
Dentyne - Fire ☒
- Ice ☒
Excel ☒
Extra ☒
Freedent ☒
Trident - pellet ☒
- stick ☒
Trident Splash ☒
Other ☒

SOY-BASED FOOD PRODUCTS

☒ WE DO NOT USE (Skip to next category)	Used in Past 12 Months	Our Usual Brand(s)
MEAT ALTERNATIVES		
Oh Nature!!	☒	☒
President's Choice	☒	☒

FREEZER



HEALTHCARE PRODUCT SAMPLES

1) Would you be interested in receiving samples and offers from Wyeth Consumer Healthcare Inc., the makers of Advil and Robitussin? If 'Yes' we will credit you a penny. (Please check one only)

Yes ☒ No ☒

2) Health Canada requires a nominal exchange of value for the distribution of healthcare product samples. Would you like to trade your penny to potentially receive a sample of Wyeth products? (Please check one only)

Yes ☒ No ☒

CHILDREN'S COLD REMEDIES

WE DO NOT USE ☒ (Skip to next category)	Used in Past 12 Months	Our Usual Brand(s)
Benylin - children	☒	☒
Children's Advil Cold	☒	☒
Children's Tylenol Cold	☒	☒
Dimetapp - children	☒	☒
Triaminic	☒	☒

the following?

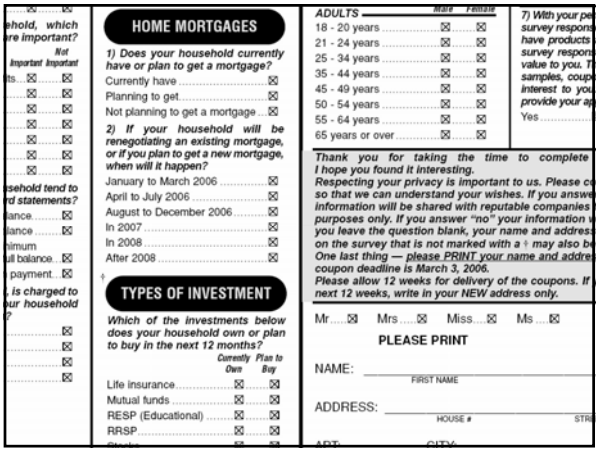
	You	Others in Household
Allergies	☒	☒
Arthritis		
- rheumatoid arthritis	☒	☒
- osteo arthritis	☒	☒
- ankylosing spondylitis	☒	☒
Asthma	☒	☒
Back pain - frequent	☒	☒
- occasional	☒	☒
Bladder leakage	☒	☒
Crohn's disease	☒	☒
Ulcerative colitis	☒	☒
Dandruff or itchy scalp	☒	☒
Dental/Orthodontic pain	☒	☒
Dentures	☒	☒
Diabetes - Type 1	☒	☒
- Type 2	☒	☒
Headaches - moderate	☒	☒
- severe	☒	☒
Lactose intolerance	☒	☒
Menstrual pain	☒	☒
Migraines	☒	☒
Minor joint pain	☒	☒
Muscle aches and body pain	☒	☒
Regularly take 3 or more prescription medications	☒	☒
Sensitive teeth	☒	☒

Pepcid Compl
Pepto-Bismol

Rolaids
Tums
Zantac 75
Store brand - ac
- ot

† Prescription re
Other - liquid
- tablets

† *How often is used in your*
Daily
4 to 6 times pe
2 or 3 times p
Once per wee
Less than onc



HOME MORTGAGES

1) Does your household currently have or plan to get a mortgage?

Currently have ☒
Planning to get ☒
Not planning to get a mortgage ☒

2) If your household will be renegotiating an existing mortgage, or if you plan to get a new mortgage, when will it happen?

January to March 2006 ☒
April to July 2006 ☒
August to December 2006 ☒
In 2007 ☒
In 2008 ☒
After 2008 ☒

† TYPES OF INVESTMENT

Which of the investments below does your household own or plan to buy in the next 12 months?

	Currently Own	Plan to Buy
Life insurance	☒	☒
Mutual funds	☒	☒
RESP (Educational)	☒	☒
RRSP	☒	☒

ADULTS	Male	Female
18 - 20 years	☒	☒
21 - 24 years	☒	☒
25 - 34 years	☒	☒
35 - 44 years	☒	☒
45 - 49 years	☒	☒
50 - 54 years	☒	☒
55 - 64 years	☒	☒
65 years or over	☒	☒

7) With your pe survey respons have products survey respons value to you. T samples, coup interest to you provide your ap

Yes

Thank you for taking the time to complete I hope you found it interesting.
Respecting your privacy is important to us. Please co so that we can understand your wishes. If you answe information will be shared with reputable companies purposes only. If you answer "no" your information you leave the question blank, your name and address on the survey that is not marked with a † may also be One last thing — please PRINT your name and addres coupon deadline is March 3, 2006.
Please allow 12 weeks for delivery of the coupons. If next 12 weeks, write in your NEW address only.

Mr. ☒ Mrs. ☒ Miss. ☒ Ms. ☒

PLEASE PRINT

NAME: _____ FIRST NAME

ADDRESS: _____ HOUSE # STR

APT: CITY:

ICOM Privacy Policy

"In general, Shopper's Voice™ collects consumer opinions, shopping habits & other related information in order to provide services of value to our individual members and partner companies.

We generally use this information in 3 ways:

- To provide members with relevant information & offers
- To help partner companies introduce new products and market existing ones
- To send members other information about Shopper's Voice

We also may use and share information as described in our Privacy Policy below….."

uOttawa
L'Université canadienne
Canada's university

Compliance with Privacy Law

1. Data collectors obtain consent from consumers/ respondents
   - Data brokers/agents rely on data owners to get consent

   Q: Is meaningful consent being obtained?

2. No consent required
   - Anonymous data only

   Q: Is the data re-personalized?

Specific Lists - USA

- Addiction Recovery Book Buyers
- Addiction Responders (email, postal, telephone)
- Tobacco Users
- Americans with depression
- Aching and Ailing
- Ailments and Health Conditions
- "My Health Factor" Ailments and Medications Masterfile
- #1 Ailment – Mental Health Disorders
- Diabetes Care Guide responders

Seasonal Affective Disorder Sufferers at Home (US)

"Company Information:
"Integrated Business Services, Inc." (IBSI) is a medical research and information marketing firm providing access to highly selectable medical databases. We are the owner of the MEDBASE200® masterfile, which this file is a subset of. These lists are made possible by conducting market analyses and surveys for this firm, as well as for corporate clients in the healthcare marketplace, and via internal file verification."

Rx Selector (US)

"The businesses challenges in the healthcare and pharmaceutical industries are numerous and complex. That's why companies turn to Equifax Rx Selector for fresh, accurate data from one of the industry's oldest consumer databases for prescription and health-related information. With data derived from millions of surveys each year, this comprehensive list includes self-reported, HIPAA compliant data on issues ranging from diabetes to digestive disorders, mental health to vascular issues and more! With over 6.5 million records attached to a wide range of demographic and interest selections, the Rx Selector is the answer to all your prospecting needs."

My Health Factor – Ailments & Medications Masterfile

These individuals have self-reported their specific health maladies and the prescription or OTC medications used for treatment. "My Health Factor" is an interactive internet resource where members provide detailed health/medical histories along with demographic information. Data collection is supplemented by third party surveys contracted to provide their proprietary health responders.

Addiction Responders (US)

"Who is struggling with an addiction to gambling, sex, or food? Who can't "just say no" to drugs, alcohol, or tobacco? Millions of American consumers, and Vente has them. Vente's Addiction Responders file has all the data you need to reach those Americans who suffer with addictions. With a consumer database of more than 30 million consumers and 4,500 selectable data points, Vente's self-reported data …

Vente, an Experian company, has the industry's largest and most comprehensive consumer database of self-reported online data, compiled from three reliable sources including online surveys, direct response e-mail marketing and consumers visiting Vente websites."

People with Ailments Masterfile (US)

"This database, containing over 39,000,000 names, was compiled from telephone and mail order purchase information, rebate coupons, prescription records, subscription order forms, warranty card registrations, sweepstakes entry forms, 800# respondents, trade show/conference attendee rosters and consumer surveys & questionnaires."

Concerns – Use of Lists

- Direct marketing
- Insurance
- Employment
- Government benefits
- Travel (border control)
- Other government uses?
- Treatment?

Concerns

- Individual Profiling
  - survey-based data brokers
  - based on multiple lists
- Accuracy of information
- Surveillance Society

www.cippic.ca

What do Canadians think about electronic health information and privacy? A systematic review of public opinion surveys and trends, 1999-2006.

Mary Lysyk, Policy Advisor, Health Canada and the University of Ottawa

Abstract:
For many years now, Canadians have been asked about their concerns about the privacy of their personal health information in electronic environments. This presentation will summarize public opinion and privacy as it pertains to personal information, personal health information, electronic health records, changes in behaviour, secondary uses of data as well as building public trust. Recommendations for future surveys will be highlighted.

Bio:
Mary is a policy analyst with the Access to Information and Privacy Policy Division, Health Canada. As well, she is completing her PhD in the Population Health Program, University of Ottawa, with a focus on electronic health information privacy for the health research community.

Slides Unavailable

Inter-jurisdictional sharing of health information among Federal, Provincial and Territorial Governments for Public Health Management

Jeannine Parent, Health Canada, Access to Information and Division

Abstract:
In the current Canadian privacy landscape, there are 23 privacy laws establishing varying degrees of privacy protection. Jurisdictional borders are not relevant to diseases. Consequently, effective information sharing between Federal, Provincial and Territorial Governments is key to the effective monitoring and management of all illnesses including communicable and chronic diseases. Notably, during a public health emergency, such as a pandemic influenza, the timely sharing of information, including personal health information, becomes critical for the management and the containment of the disease to assure the safety and health of all Canadians. This presentation will examine Federal, Provincial and Territorial privacy legislation, and some of the issues surrounding the sharing of health information between Canadian Governments for public health management.

Bio:
Jeannine Parent is currently a Senior Privacy Policy Advisor and the Privacy Impact Assessment Coordinator at Health Canada. In 2005 she was seconded for one year to the new Public Health Agency of Canada as the Team Leader, Information Sharing Policy and Privacy. In this capacity, she led the development of a Federal/Provincial/Territorial framework for the sharing of health information for public health surveillance purposes. Prior to this appointment, Jeannine was Health Canada's lead Advisor for the development of the Pan-Canadian Health Information Privacy and Confidentiality Privacy Framework and also led the Government of Canada's PIPEDA Awareness Raising Tools (PARTs) Initiative. She holds a law degree from the University of Ottawa and has over 20 years experience in information and communications technologies. Prior to joining the Government of Canada, she held various management positions within the IT industry in marketing and tele-healthcare application development. She has been a guest speaker at numerous national and international workshops and conferences.

Health Canada Santé Canada

Inter-jurisdictional Sharing of Personal Information for Public Health Management

Electronic Health Information & Privacy Conference
November 13, 2006

Jeannine Parent,
Access to Information and Privacy Division,
Health Canada

Canada

Health Canada Santé Canada

Overview

- Introduction
- Public Health and Health Care
- Privacy Considerations in Public Health
- Pan-Canadian Health Information Privacy and Confidentiality Framework and PH
- Thank you!

Canada

Health Canada Santé Canada

Health Care System & Public Health System are they the same?

- Health Care:
  - the system of hospitals, doctors, nurses and other professionals to whom we turn when we are sick or injured.
- Public Health:
  - The system that is responsible for helping protect Canadians from injury and disease and for helping them stay healthy. Its focus is prevention.

Canada

Health Canada Santé Canada

How Does Surveillance Work?

1. Data collection on a specific health event, risk factor or exposure

Risk Factors — Health Event — Exposures

2. Integration of relevant information

PHI — Environmental Reports — Laboratory

3. Analysis by health professionals

4. Interpretation of the data by health professionals

For use as:
- Alerts (SARS)
- CD notification
- Applied research

5. Dissemination of information

6. Action

Health policy & programs

Outbreak management

Health Canada Santé Canada

Privacy Considerations in Public Health

- Privacy is recognized as a fundamental human right
- Canadians are generally more concerned about the privacy of their health information than other types of personal information
- Canadian Governments' privacy measures must meet legislative requirements and continue to assure the public that their privacy is protected
- Governments must balance the rights of individuals with the rights of the collective Canadian population

Health Canada Santé Canada

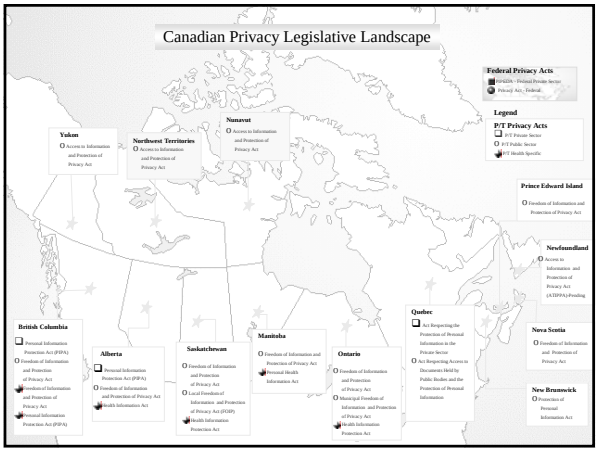
Why is privacy so important now?

- Increased public awareness
- Evolving technologies
- Increased sensitivity of health information

Health Canada Santé Canada

Privacy Legislative Landscape

- Canadian Charter of Rights and Freedoms
- La Charte des Droits et Liberté de la Personne du Québec
- Privacy Act
- Access to Information Act
- PIPEDA
- Freedom of Information & Privacy Acts
- Provincial Health Information Acts
- Library and Archives of Canada Act
- Federal, Provincial and Territorial laws pertaining to Public Health



Health Canada Santé Canada

Personal Information

It is information about an **identifiable** individual

- Ethnic origin, colour, religion, age or marital status
- Education, medical, criminal or employment history
- Identifying number (SIN, medicare, PRI)
- Address, finger prints or blood type
- The personal opinions about you expressed by another individual

Health Canada Santé Canada

Personal Health Information

It is information about :

- the physical or mental health of an identifiable individual, or
- the provision of health services including:
  - registration of the individual
  - payments or eligibility for health care
  - a unique identifier
  - information collected for the provision of health
  - services, and
  - information derived from a body part or bodily substance.
- **Does not** include information that, either by itself or when combined with other information is anonymized, i.e. the identity of the individual who is the subject of the information cannot be readily ascertained from the information

Health Canada Santé Canada

How do I exercise my right to Privacy?

- Consent!
  - Collection
    - Public sector privacy laws
    - Private sector privacy laws
    - Health information privacy laws
  - Use
  - Disclosure
- Exceptions

Health Canada Santé Canada

Consent in a Public Health Context

- Public Health Emergency
  - International Health Regulations (WHO)
- Communicable Disease Surveillance
- Chronic Disease Surveillance
- Injury Surveillance

Health Canada Santé Canada

Inter-jurisdictional Sharing of Personal Information for Public Health

- With the concerned individual's Consent
- Without the concerned individual's Consent
  - When authorized by law
  - When required by law
  - When it is in the public interest or if there is a significant risk of harm to the health or safety of an individual or a group of people

Health Canada Santé Canada

Pan-Canadian Health Information Privacy and Confidentiality Framework

- Set of harmonized principles and provisions for the collection, use, disclosure and protection of personal health information on topics, such as:
  - **Consent**
  - **Privacy Impact Assessment**
  - **Cross Border Transfer of Personal Health Information**
  - **Public Health Surveillance**

Health Canada Santé Canada

Thank You!

Jeannine Parent
Senior Privacy Policy Advisor/PIA Coordinator
Access to Information and Privacy Division
Health Canada
Jeannine_parent@hc-sc.gc.ca
http://hc-sc.gc.ca/ahc-asc/activit/atip-aiprp/priv/index_e.html

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

Inter-Jurisdictional Sharing of Information During a Public Health Emergency – A Canadian Perspective

Electronic Health Information & Privacy Conference

André La Prairie
Office of Public Health Practice
Public Health Agency of Canada

Ottawa–-November 2006

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

Public Health

P	Health Promotion Disease Prevention Injury Prevention
p	Protection Population Health Assessment Health Surveillance

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

Jurisdiction over Public Health

***Constitution Act*, 1867**

Federal

- Criminal Law
- Quarantine and Marine Hospitals
- Peace, Order and Good Government
- Spending Power
- Navigation and Shipping
- Indians / Lands Reserves
- Trade & Commerce

Provincial

- Local or Private Matters
- Property & Civil Rights
- Establishment of Hospitals
- Education
- Spending Power
- Municipal Institutions
- Local Works

Organization of PH in Canada

- Population (2006 est.): ~ 33 million
- Land Area: ~ 10 million km^2
- 14 administrative divisions: Federal (1); Provinces (10); Territories (3)
- ~140 local/regional PH units serving populations of different sizes (600-2.4M) and areas (4-800,000 km^2)
- Entities dedicated to PH in some jurisdictions
  - *Institut national de santé publique du Québec*
  - *British Columbia Centre for Disease Control*
  - *Ontario Health Protection and Promotion Agency*
  - *Public Health Agency of Canada*

Public Health Agency of Canada

Mission: To promote and protect the health of Canadians through leadership, partnership, innovation and action in public health.

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

Pan-Canadian PH Network

- "New" intergovernmental mechanism to:
  - Support PH challenges jurisdictions face during emergencies;
  - Collaborate on the day-to-day operations of PH;
  - Provide advice/regular reporting to jurisdictions on PH matters and the activities of the Network; and
  - Facilitate information sharing among all jurisdictions and disseminate information regarding best-practices in PH.
- Web site: www.phn-rsp.ca

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

Lessons from SARS

shared responsibility…

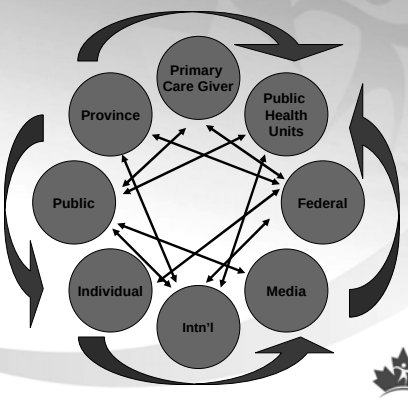
PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

Lessons from SARS

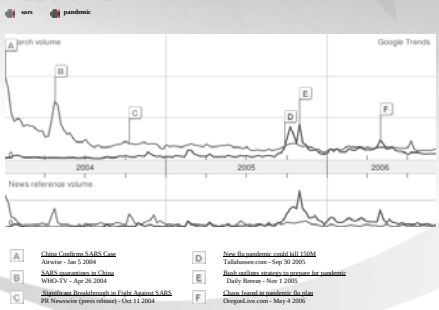
"What is striking from all this is that the various groups appear honestly to believe that they communicated the information to each other. Yet clearly there were significant gaps in the transfer of information between Toronto Public Health and the province, between the provincial Epi Unit and the Science Committee, and between Ontario and the Federal government. …..The bottom line is that the lack of clarity around the flow of communication and the reporting structure, the absence of a pre-existing epidemiological unit coordinated with the local health units and the absence of clear public health leadership above the Epi Unit provided an environment in which the crucial elements of the fight against SARS were disconnected from each other. ."

THE SARS COMMISSION INTERIM REPORT April 15, 2004

Info Flows



Lessons from SARS

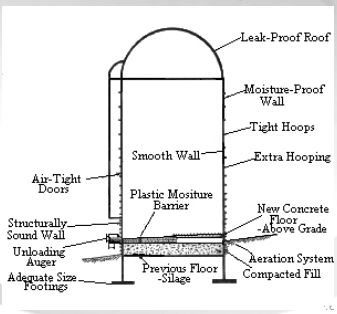


A China Confirms SARS Case — Airwise - Jan 5 2004
B SARS quarantines in China — WHO-TV - Apr 26 2004
C Significant Breakthrough in Fight Against SARS — PR Newswire (press release) - Oct 11 2004
D New flu pandemic could kill 150M — Tallahassee.com - Sep 30 2005
E Bush outlines strategy to prepare for pandemic — Daily Breeze - Nov 1 2005
F Chaos feared in pandemic flu plan — OregonLive.com - May 4 2006

From « Silos » to « Systems »

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

From « Silos » to « Systems »



PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

From « Silos » to « Systems »

Information Sharing Initiative

- Principles for Public Health Information Sharing
- Processes for Sharing Information during a Public Health Emergency
- Detailed business processes/information flows (communicable diseases)
- « Model » Agreement, with implementation strategy/plan

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

From « Silos » to « Systems »

Current Activity

- Protocols/processes for declaring that a Public Health Emergency exists and when it ends.
- Protocols/processes for the notification of Jurisdictions, National coordinating bodies, Foreign National / International Health Regulation Focal Points and the WHO during a Public Health Emergency.
- Strategies to address potential legal, regulatory and policy constraints to information sharing during a Public Health Emergency.
- Definitions, protocols, guidelines and agreements to share information between and among Jurisdictions and a communication strategy to ensure effective implementation.

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

Enabling Legal Authorities

- During a public health emergency, authority of jurisdictions to
  - collect health information originating from outside of their jurisdiction
  - use this information within their jurisdiction
  - disclose information originating from within their jurisdiction to other jurisdictions
- Authority of institutions to engage in the above activities without an individual's consent

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

International Health Regulations

With permission, WHO

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

Do pathogens have passports?

With permission, WHO

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

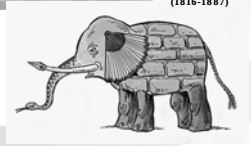
The Blind Men and the Interoperable Elephant

And so these men of Indostan, Disputed loud and long, Each in his own opinion Exceeding stiff and strong,

Though each was partly in the right, And all were in the wrong!

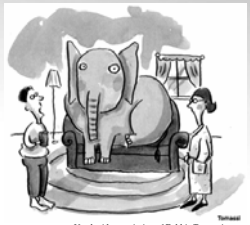
Blind Men and the Elephant.

John Godfrey Saxe (1816-1887)



PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

The elephant in the room



Used with permission of Debbie Tomassi

The moose under the table

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA


Economist.com

Is your business

Science & Technology

Global health

A shot of transparency

Governments have been reluctant to share information about possible pandemics of disease. Happily, that is changing

"FOR the sake of basic human interests, the Indonesian government declares that genomic data on bird-flu viruses can be accessed by anyone." With those words, spoken on August 2nd, Sri Fadilah Supari started a revolution that could yet save the world from the ravages of a pandemic disease. That is because Indonesia's health minister has chosen a weapon that may prove more useful than today's best vaccines in tackling such emerging threats as avian flu: transparency.

"Some believe that full disclosure could cause locals to panic and foreign tourists to stay away. … fear of losing exports is another factor.
The least defensible motive is vanity. Individual researchers, academic institutes and even national governments want the glory and research funding that come with solving the puzzle of a new pandemic and being first to publish. "

The Economist Aug 12, 2006

PUBLIC HEALTH AGENCY of CANADA | AGENCE DE SANTÉ PUBLIQUE du CANADA

André La Prairie
Office of Public Health Practice
Public Health Agency of Canada
E-mail: andre_la_prairie@phac-aspc.gc.ca
Web site: www.phac-aspc.gc.ca/php-psp/

“Sorry, You Can’t Have That Information” Stakeholder Awareness, Perceptions and Concerns Regarding the Disclosure and Use of Personal Health Information

Daryl Pullman, PhD, Associate Professor of Medical Ethics, Memorial University of Newfoundland
Angela Power, BA, Diploma in Applied Ethics Access and Privacy Supervisor Population Therapeutics Research Group, Faculty of Medicine, Memorial University of Newfoundland

Abstract:
Among the untoward consequences of the introduction of privacy legislation in the United States (HIPAA 1996), a key concern has been that barriers have been created for health research (Hiatt, 2003). One reason is that data stewards, research ethics boards, and institutions that collect health information have struggled to determine what data can or should be shared between institutions and with researchers (Kulynych and Korn, 2003; Fitzmaurice, 2003; Annas, 2002). Furthermore, the tension between an individual’s right to privacy and the broader public good accomplished through public health research admits of no easy solutions (Califf and Muhlbaier, 2003; Jepson and Robertson, 2003; Menzel, 2003). Regulators and research ethics boards in the U.K., for example, have been criticized for giving undue weight to the privacy of the individual (Kent, 2003).

The purpose of this project is to assess stakeholder awareness, perceptions and concerns regarding the collection, use, and disclosure of personal health information for the purpose of health research. While studies conducted in other jurisdictions have focused primarily on the public (Government of Canada, March 2003; GPC Alberta 2003), or upon specific stakeholder groups affected by the emerging privacy regimes at both the national and provincial levels (Willison et al, 2003; Health Canada Vision 2020 Workshops, 2000), this project aims to assess a wide range of stakeholders including the general public, health researchers, physicians, pharmacists, nurses, social workers, as well as custodians of information databases and data stewards. Our aim is to determine the relative level of familiarity among these groups with regard to current privacy legislation and regulations, and to assess the degree to which different stakeholder groups express similar or quite different concerns regarding the health information they can either access or share for research purposes.

Both quantitative and qualitative methodologies have been employed in this study, and a variety of instruments have been developed and administered. A survey instrument was developed for the public consultation, and was administered through random digit dialing to a representative sample of rural and urban, as well as male and female residents of the province. A revised survey that reflects specific stakeholder contexts and issues was also administered to pharmacists, physicians, social workers, nurses, health researchers and database managers. After initial assessment of the survey data, focus groups were performed with each stakeholder group.

Bio:
Daryl Pullman is a philosopher-bioethicist who has worked extensively in the area of research ethics. He is centrally involved in the current provincial initiative to introduce legislation to govern all health related research conducted in the province, and has advised the government on the regulation of commercially sponsored genetic research. As a member of the Ethics Oversight Committee of the Canadian Life Long Health Initiative he is involved in exploring and monitoring issues regarding privacy that have some parallels to the current project. He is a co-investigator (responsible for ethics) on the Population Therapeutics Research Group (PTRG). It is expected that knowledge gained from this project will inform key policy and procedural issues related to the development and utilization of the PRD.

Angela Power is the Access and Privacy Supervisor with PTRG, working on the Pharmacy Research Database project, the Heritability Analytics Infrastructure
(HAI) project and the affiliated Privacy project. Angela has extensive experience with qualitative and quantitative social science research, both within and outside the healthcare setting. She is completing an Information Access and Protection of Privacy Certificate from the University of

Alberta and is currently responsible for developing PIA guidelines as a secondary user of electronic record sources.

Managing Security Incidents involving personal information: What to do when the unthinkable occurs

Michael Power, Partner and Chief Privacy Officer, Gowlings Lafleur Henderson LLP

Abstract:
PHIPA requires a health information custodian that has custody or control of personal health information about an individual to notify the individual at the first reasonable opportunity if the

a1

Privacy Study

Sorry, You Can't Have That Information: Stakeholder awareness, perceptions and concerns regarding the disclosure and use of personal health information (PHI)

Principal Investigator: Dr. Daryl Pullman

Memorial University of Newfoundland

CIHR IRSC

Presentation Overview

- Study Design
- Results
  - Awareness of Privacy
  - Safety and Security of PHI
  - Research Using PHI
- Limitations
- Conclusions
- Discussion points

Presentation Overview

- **Study Design**
- Results
  - Awareness of Privacy
  - Safety and Security of PHI
  - Research Using PHI
- Limitations
- Conclusions
- Discussion points

Study Objectives

- Assess awareness, perceptions and concerns regarding the collection, use, and disclosure of personal health information *for health research*
- Understand perspectives of various stakeholders
- Assess perceptions on balance between information access (research) and privacy protection

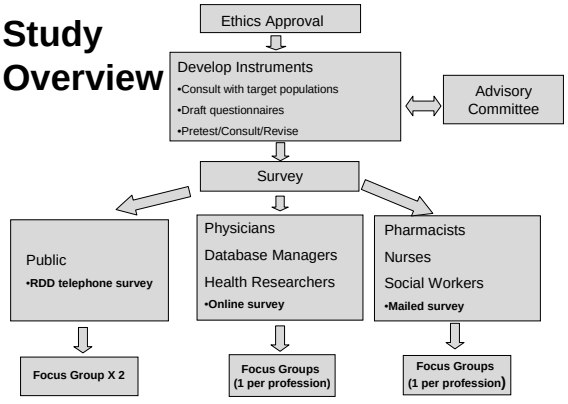
CIHR IRSC

Methodology

Survey with follow-up focus groups

- Survey
  - Questionnaire developed in consultation with stakeholder representatives
    - Some adjustment for population experience
  - Included scenarios to help focus the questions
  - Survey administered via:
    - Random digit dialing (Public)
    - On-line (Physicians; Health Researchers; Data base Managers)
    - Mail-out (Pharmacists; Nurses; Social Workers)
- Focus Groups

Study Overview



Our Stakeholders

A real *Steak-holder*

- Public
  - Rural/Urban; Male/Female
- Professional Groups
  - Physicians
  - Pharmacists
  - Nurses
  - Social Workers
  - Database Managers
  - Health Researchers

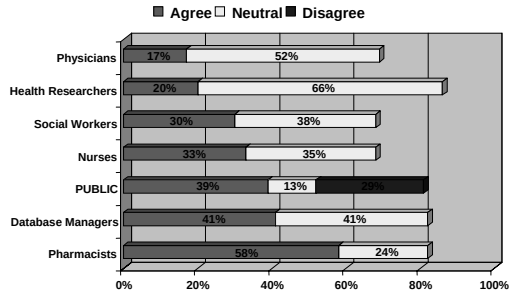
Response Rates

- Public **72%** (623/862 contacts)
- Physicians **14%** (100/719)
- Pharmacists **12%** (67/540)
- Social Workers **21%** (231/1080)
- Nurses **55%** (513/926)
- Database Managers **33%** (23/69)
- Health Researchers **22%** (47/214)

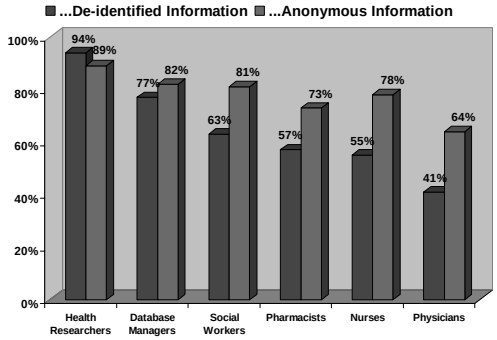
Presentation Overview

- Study Design
- **Results**
  - **Awareness of Privacy**
  - Safety and Security of PHI
  - Research Using PHI
- Limitations
- Conclusions
- Discussion points

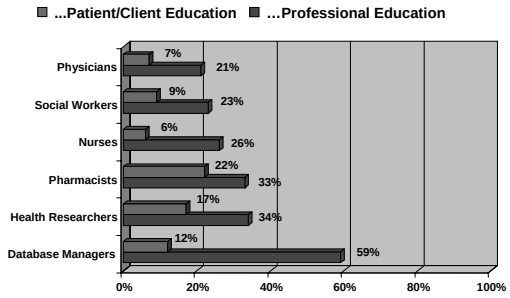
The province is doing enough to protect and safeguard individuals' PHI…



I understand the meaning of …



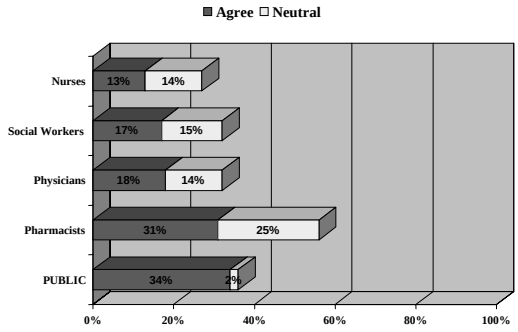
Education: Enough has been done to improve…



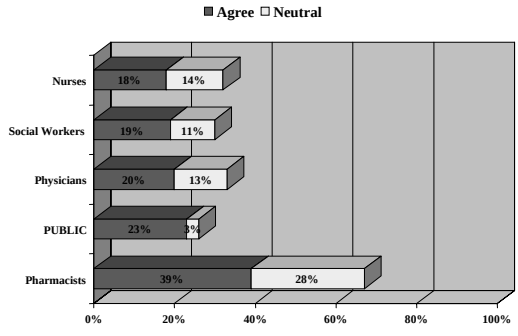
Presentation Overview

- Study Design
- **Results**
  - Awareness of Privacy
  - **Safety and Security of PHI**
  - Research Using PHI
- Limitations
- Conclusions
- Discussion points

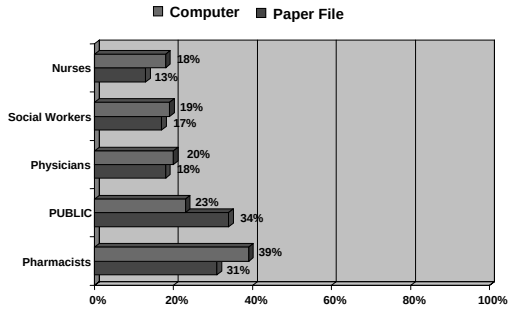
Agree that PHI stored in paper file is safe and secure



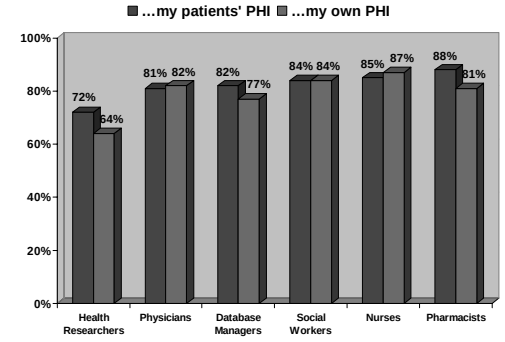
Agree that PHI stored in computer is safe and secure



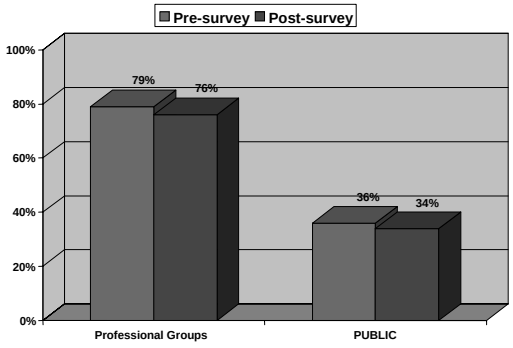
Agree that PHI stored in (i) computer or (ii) paper file is safe and secure



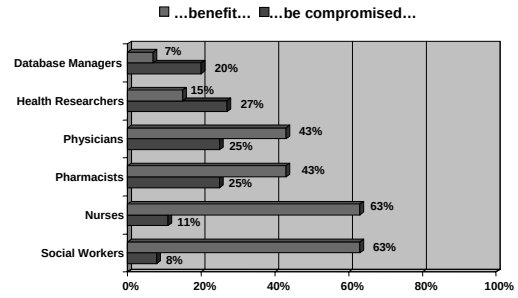
I am concerned about the privacy & security of (i) my patients' PHI or (ii) my own PHI



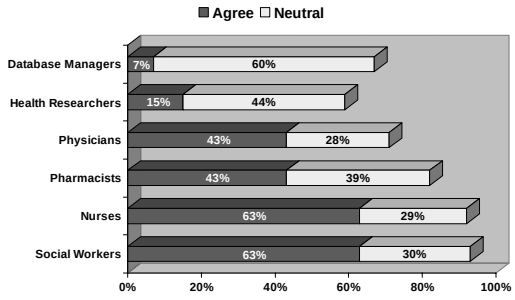
I am concerned about the privacy & security of my own PHI



The health system as a whole would (i) benefit or (ii) be compromised if there was <u>increased control</u> over privacy of PHI used in research



The health system would benefit if there was <u>increased control</u> over privacy of PHI used in research



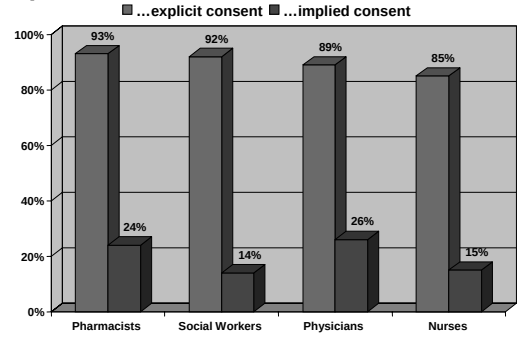
"But the system is never going to go forward unless you can get information out and get it analyzed and if everyone stays in their own little box, you might get very private but there's not going to be much progress made."

-Member of General Public

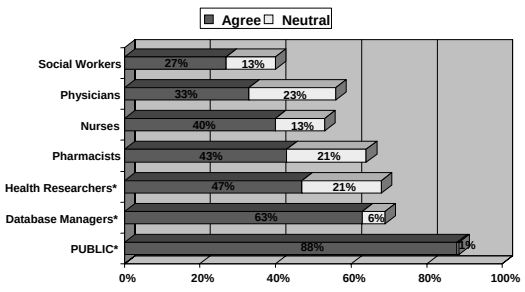
Presentation Overview

- Study Design
- **Results**
  - Awareness of Privacy
  - Safety and Security of PHI
  - **Research Using PHI**
- Limitations
- Conclusions
- Discussion points

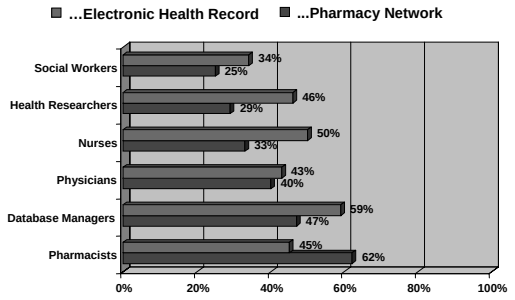
It is okay to share patients'/clients' PHI if I have their (i) explicit consent or (ii) implied consent



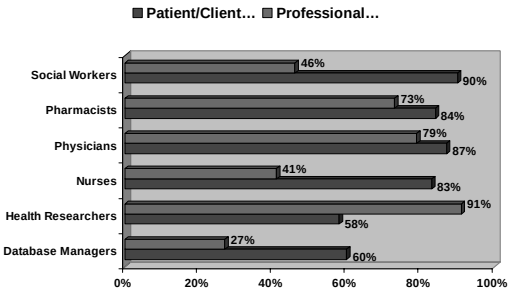
It is okay for researchers on a NEW study to look at "de-identified" information from a previous study without re-consent



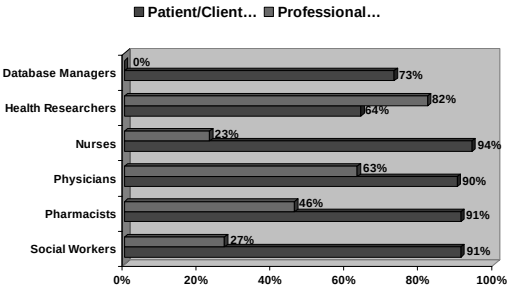
I am familiar with the proposed…



Who should control access to the PHI you collect?



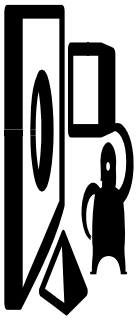
Who has a degree of ownership over the PHI collected by you?



Presentation Overview

- Study Design
- Results
  - Awareness of Privacy
  - Safety and Security of PHI
  - Research Using PHI
- **Limitations**
- **Conclusions**
- **Discussion points**

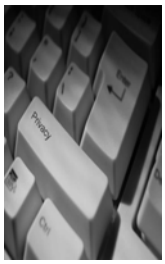
Limitations



- Survey methods varied
- On-line respondents (physicians; database managers; researchers) could not go back to change/correct responses
- Phrasing of some questions needed to be altered to accommodate specific audience
- Small sample size for some groups (pharmacists; physicians)

Conclusions

- Professional groups in general lack a clear understanding of their privacy and security obligations with regard to PHI
  - ***"You need to put out a lot on privacy education because a little bit of information can be a really dangerous thing and people start to get really upset."-Pharmacist***
- In general the public is not as concerned about the privacy of their PHI as are the professionals who control access to it
- Professional groups display ambivalence with regard to how privacy and access concerns might impact upon health research



Discussion points

- Lack of understanding of privacy requirements may lead to conservative practices with regard to sharing of PHI
  - ***"It's sort of like, wow, we're being told now that we might actually be liable for something if we shared some kind of information that seems innocuous, so when in doubt, don't."*** *-Health Researcher*
- Professionals are generally unsure of how to interpret and apply privacy legislation in their work settings
  - ***"One of the big causes of medical errors is lack of communication, but it seems that privacy…this whole privacy thing will decrease communication in some instances."-*** *Physician*

Privacy Research Team

Dr. Sharon Buehler — *Community Health & Humanities*
Dr. Larry Felt — *Sociology*
Dr. Katherine Gallagher — *Business*
Ms. Jeannie House — *Regional Health Boards*
Mr. Montgomery Keough — *Health Research Unit*
Ms. Lucy McDonald — *Newfoundland & Labrador Centre for Health Information*
Ms. Angela Power — *Population Therapeutics Research Group/ Newfoundland & Labrador Centre for Health Information*
Ms. Ann Ryan — *Health Research Unit*
Dr. Roy West — *Community Health & Humanities*

Managing Security Incidents involving personal information: What to do when the unthinkable occurs

Michael Power, Partner and Chief Privacy Officer, Gowlings Lafleur Henderson LLP

Abstract:
PHIPA requires a health information custodian that has custody or control of personal health information about an individual to notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons. How can organizations manage such incidents? This session will provide practical advice as to how best to comprehensively manage a security incident as well as consider evidentiary and media issues should the unthinkable occur.

Bio:
Michael Power, a partner in the Ottawa office of Gowling Lafleur Henderson LLP, provides strategic and legal advice to public and private sector clients in the areas of privacy, information technology security and electronic government. Mr. Power also serves as Gowlings' Chief Privacy Officer. He currently is a member of the National Executive of the Privacy Law Section of the Canadian Bar Association; the Canadian Information Technology Law Association, and the American Bar Association's Cyberspace Law Committee.

Michael Power received his LL.B and M.B.A. from Dalhousie University in 1983. He was admitted to the Nova Scotia Barristers Society in 1984 and the Law Society of Upper Canada in 1991.

Prior to joining Gowlings, Mr. Power held various positions within the Department of Justice, Treasury Board of Canada Secretariat and the Department of Foreign Affairs and International Trade, which included responsibilities for legal advice, policy development and issue management pertaining to information technology, electronic commerce and international trade and investment issues.

He recently collaborated in writing "Sailing in Dangerous Waters: A Director's Guide to Data Governance" to be published by the American Bar Association in August 2005.

Managing Information Security Incidents
November 2006

The Ingenuity of the Truly Determined…

- Actors
  - Disgruntled (ex)employees of
    - Organization
    - Outsource partners/consultants
  - Employees following inadequate policy and/or procedure (e.g. data destruction)
  - Criminals
    - Theft of physical property (servers, hard drives)
    - Extortion
    - Fraud (scams, phishing)

Incident Management

- Why care?
  - Media Attention
  - Regulatory Violations
  - Legal Liability
  - Financial damage to revenue/share values
- Timeframes
  - Short term
    - Contain damage
    - Restore normal operations
  - Long term
    - Avoid problem in future

The Rabbit and the Fence

- A story about failing to fix holes in the fence, and finding no rabbit tracks in the garden.
- The Players
  - **Acxiom:**
  - US Commercial data broker
  - Analyzes data on 95% of US households
  - Clients include credit card issuers
  - **Scott Levine**,
  - charged with over 100 counts associated with computer attacks on Acxiom. Levine was associated with Snipermail.com, which is now defunct, and was convicted.
  - **Snipermail**
  - Accused of conspiring to download personal records of **1.6 billion** persons from Acxiom server (in 2002 - 2003)

The Rabbit and the Fence

- ***Caveat: Based on Wall Street Journal Report of 1 August 2005***
- Acxiom:
  - Saved **all** passwords to **one** file ("PassFile")
  - Stored PassFile on **one** server
  - **Excluded** server from IT system's "firewall"
  - Server easily accessible from Internet
  - Intrusion detection system, if any, incapable of detecting unauthorized:
    - Access to server
    - Access to PassFile
    - Download of PassFile

The Rabbit and the Fence

- **What (reportedly) happened…**
  - Snipermail personnel downloaded PassFile
  - Unscrambled 40% of the passwords
  - With passwords, accessed clients' data
  - Year later, Acxiom subcontractor employee arrested for illegal download of data from Acxiom's server
  - Acxiom unaware of breach and data theft
  - Acxiom then checked: detected intrusions of same server, traced to Snipermail
  - Downloads included data from **Citicorp** and **JP Morgan Chase**

Legal Risks

- **Privacy Laws**
  - **Notification Requirement, Canada**
    - **PHIPA**
  - **Notification Requirements, United States**
  - **Appropriate Security**
    - **PIPEDA, PIPAs:**
    - **International: HIPAA, Europe, Australia, Japan**
- **Contractual Requirements (NDAs, Supplier Compliance)**
- **Fiduciary Duty of Care**
- **Evidence/"Litigation Hold" Orders**

American Notification

- Last count: some 40+ states had notification requirements
- California
  - The precedent: Immediate notice unless data encrypted
- Threshold
  - Decision to notify may linked to degree of harm
- Delays
  - Law enforcement intervention permitted
- Consumer Protection
  - Notice required to be sent to Consumer Reporting Agencies
- Problem: Hard to know if *access* occurred.

PHIPA

- S.12(2)
- Provision elements
  - HIC
  - Custody or control
  - PHI
  - Notify
  - Individuals
  - 1st reasonable opportunity
  - Stolen, lost or accessed
- Recommendation: When in doubt, talk to IPC.

Incident Management Process

- Discover
  - Assemble team
  - Activate plan
- Triage
  - Assess seriousness
- React
- Communicate
- Repair

Resource Incidents Properly

- Assign project manager.
- Contact lawyers:
  - Evidence;
  - Employment Issues .
- Retain media advisors.
- Define project team.
- Define liaison (management and service provider, if applicable) and reporting requirements.
- Did we mention retain lawyers and media advisors (Not a typo but really, really good idea).

Decisions

- Who needs to know?
  - Customers
  - Regulators
  - US (general)/Ontario (health)
- When?
  - Minor incident?
  - Identity Theft?
- How?
  - Media?
  - Correspondence?
- Be candid and proactive

Messages

- The simplified facts
  - What happened.
- The Speed of Discovery and Reaction
  - How we discovered it and what we did.
- Triage and Containment Measures
  - What we're doing now.
- Preventative Measures
  - What we're going to do to make sure this doesn't happen again.
- Contact/Communication details
  - How you can get more information.

Problem…People

- No "ands, ifs or buts"
  - Some people get really upset.
  - Some people you can't "manage".
  - Some people won't understand.
- Simply give them an outlet:
  - Send them to Privacy Officer or Privacy Commissioner.

Service Providers

- Outsourcing
  - May cause delay in response
  - Requires provider and client to be on same page
  - Need to anticipate responding to incidents
  - Need to coordinate media responses
  - Ensure outsourcing agreement addresses subject of incidents
    - Mandatory reporting of incidents
    - Right of audit
    - Prompt/periodic identification of subcontractors

Communications

- After lawyer, retain media advisor (3rd mention)
- Plan communications
  - Prepare
    - Executives for media
    - Response staff for customers
    - FAQ for general use
- *Mea Culpa* works
- Where possible, personalize messages
- TIME IS OF THE ESSENCE

CONCLUSIONS

- Proactive approach works best
- As does honesty
- Bottom line:
  - Incidents result in lost trust – need to earn that trust back
  - Communications key to building trust

Thank You

Michael Power
613.786.8685
michael.power@gowlings.com

Applications of Data Masking Technology in Practice

Paul Preston, Plato Group Inc.

Abstract:
Information is one of an organization’s most valuable assets, however, unless properly protected, it can also be a significant liability. Many organizations create copies of production databases for use in non-production environments, and these copies are oftentimes less protected than production data, exposing sensitive information to insiders. Traditionally, organizations have been concerned with protecting this sensitive data from external theft. However, as research indicates, more than 80% of security incidents come from insiders. The emergence of several trends such as the increase in electronic data captures, data mining, and outsourcing have drastically changed how organizations handle personal and sensitive data. Combined with an increase in data theft and strict privacy legislation, these worldwide trends drive the need for organizations to augment conventional security mechanisms to protect their valuable data.

Bio:
Paul Preston is the Director of Business Development with Plato. He is responsible for strategy creation, business development activities, and client management for the company's data masking software Camouflage®. As part of his role, he is involved with Camouflage® development initiatives from a functional and technical perspective. He has a Masters of Business Administration from Memorial University, as well as a Bachelor of Commerce focused in Human Resources Management. Before joining Plato, Paul spent several years working within the Human Resources Management field of government and taught part-time at the post secondary level. In his extra time, Paul has held volunteer executive positions with several privacy and professional associations.

Data Masking

Counter Attack to Identity Theft

Camouflage

Agenda

- Data Privacy
- Legislative Environment, Data Theft, and Research Findings
- Data Masking Defined
- Business Case and ROI
- Data Masking Requirements
- Data Masking Model
- Comments and Discussion

Camouflage

Data Privacy

- Definition
  - the relationship between technology and the expectation of privacy in the collection and sharing of personally identifiable information
  - Includes: names, SSNs, addresses, phone numbers, credit card #s, financial records, medical records, etc.
  - Information is an organization's most valuable asset

Camouflage

Growth in Data Privacy

- Global Trends:
  - Heightened privacy concerns
  - New privacy legislation & regulations
  - Increase in data theft
  - Increase in data privacy security spending
  - Trend in data mining and information sharing
  - Trend towards outsourcing & offshoring

Privacy Concerns

- Consumers are increasingly concerned with the protection of their personal information
  - Approximately 64% of consumers ranked data privacy as their greatest fear worldwide; surpassing environmental degradation, terrorism, job loss, disease, etc.
- Information security ranked as the most important technology issue in the *2006 AICPA's Top Ten Technologies Program*

Healthcare Privacy Concerns

- Between February 2005 and June 2006, medical organizations accounted for 11% of worldwide data breaches

The California Healthcare Foundation

- 67% of Americans are concerned with the protection of their medical related information
- 59% of Americans recall receiving notices for privacy breaches of their medical information

Worldwide Legislative Environment

- Gramm-Leach-Bliley Act (US)
- Sarbanes Oxley Act (US)
- The Fair and Accurate Credit Transaction Act (US)
- California Senate Bill 1386 (US)
- Privacy Act (Canada)
- Australian Privacy Act 1988 (Privacy Amendment Act of 2003)
- European Union Privacy Act (EUPA)
- Japanese Personal Information Act 2003 (JPIPA)

- As of July 2006:
  - 34 American state data breach notification laws
  - 25 American credit card security freeze laws

Camouflage

Health-Related Privacy Legislation

National Legislation

- Health Insurance Portability and Accountability Act (US)
- Personal Information Protection and Electronic Documents Act (Canada)

Canadian Provincial Legislation

- Alberta - *Health Information Act*
- Saskatchewan - *The Health Information Protection Act*
- Manitoba - *Personal Health Information Act*
- Ontario - *Personal Health Information Protection Act*
- Quebec - the *Public Sector Act* & the *Private Sector Act*

Camouflage

Health Insurance Portability and Accountability Act (HIPAA)

- Enacted by the US Government in 1996
- Includes standards for collecting, storing, and sharing Protected Health Information (PHI)

Protected Heath Information (PHI) includes data that links an individual to his/her:

- Health status
- Provision of healthcare
- Health care payments

Camouflage

Health Insurance Portability and Accountability Act (HIPAA)

- The Security Rule of HIPAA (2003) ensures that organizations must:
  - Restrict access to PHI only to individuals who need it to complete their job duties and responsibilities
  - Protect information systems that contain sensitive information from intrusion

Personal Information Protection and Electronic Documents Act (PIPEDA)

- Established in Canada to regulate the collection, storage and disclosure of personally identifiable information in the private sector
  - Organizations must ensure:
    - Information is only used and disclosed for the purpose for which is was originally collected
    - Adequate information system security and data protection
- In 2002, the scope of PIPEDA expanded to include the Canadian Health Sector
  - Regulates Personal Health Information (PHI)

Insider Attacks

- *Accenture and InformationWeek*: Security breaches are increasingly coming from the inside
- *Gartner:* 70% of all security incidents come from insiders
- *Forrester:* 80% of threats come from insiders and 65% are undetected
- *Ernst & Young:* An insider attack against a large company causes an average of $2.7 million US in damages, where the average outside attack costs only $57,000 (*Almost 50 times as costly)*

Data Masking Defined

- Conventional Security Measures:
  1. Encryption: protects data while at rest
  2. Firewalls & Passwords: protect data from external threats
- Emerging Security Measure – *Data Masking:*
  - *Data Masking* is another needed solution for data protection from both internal and external security threats
  - Also referred to as data obfuscation, data de-identification, data depersonalization, data scrubbing, data scrambling, etc.

Camouflage

Data Masking Defined

- The process whereby the information in a database is masked or 'de-identified'
- It enables the creation of realistic data in non-production environments without the risk of exposing sensitive information to unauthorized users
- Data masking ensures the protection of sensitive information from a multitude of threats posed both outside and inside the organization's perimeter

Camouflage

Data Masking Defined

- Non-production environments are vulnerable to security threats from insiders who do not have 'need to know access'
- Data Masking is used in non-production environments for purposes such as:
  - Software development & implementation testing
  - Software user training
  - Data mining/research
  - Outsourcing and offshoring

Camouflage

Data Masking Defined

- Unlike encrypted data, masked information maintains it's usability for activities like software development and testing
- Encompass a number of techniques:
  - Mutation
  - Generation
  - Algorithmic
  - Loading
  - Customization

Camouflage

Data Masking Best Practices

First & Last Name	Shuffle
Address	Linked Shuffle
Phone Number	Random Number Generator or Replace
Date	Date Transformer or Date Generator
Email Address	Combo
Account Number	Account Generator
Social Security Number	National ID Generator
Medical Record Number	Random Number Generator or Account Generator
Health Plan ID Number	Account Generator

Camouflage

Benefits of Data Masking

- Increases protection against data theft
  - Enforces 'need to know access'
  - Researchers in 2006 found that almost 80 to 90 percent of Fortune 500 companies and government agencies have experienced data theft
- Reduces restrictions on data use
- Provides realistic data for testing, development, training, outsourcing, data mining/research, etc.

Camouflage

Benefits of Data Masking

- Enables off-site and cross-border software development and data sharing
- Supports compliance with privacy legislation & policies
  - Data masking demonstrates corporate due diligence regarding compliance with data privacy legislation
- Improves client confidence
  - Provides a heightened sense of security to clients, employees, and suppliers

Business Case and ROI

- Business Case and ROI typically based on risk mitigation factors such as:
  1. Civil Lawsuits
  2. Business Expenditures and Legal Fines
  3. Personal Risks
  4. Loss of Clients

Business Case and ROI

1. Civil Lawsuits
   - Litigation & defense costs
   - Effort & time for preparation of defense
2. Business Expenditures & Legal Fines
   - Insurance
   - Auditing expenses
   - Detection & notification costs
   - Payouts to affected consumers

Business Case and ROI

3. Personal risks
   - Individuals within the organization may be faced with potential jail time, salary cutbacks or job loss
4. Loss of clients
   - Negative publicity
   - Damaged brands
   - Tarnished corporate image
   - Approximately 40% of Americans will terminate their relationship with an organization that experiences data theft

Camouflage

Business Case and ROI

- How do we quantify the ROI of a masking solution?

1. Rely on an estimate of risk mitigation cost savings:
   - Look at industry benchmarks
   - Understand how breaches impact other businesses within your industry
   - Balance against probability of breach
2. Factor in savings associated with less restrictions on masked data use:
   - Pursue offshore and outsourced opportunities that provide cost savings and value
   - Allow employees, contractors, third parties, etc. to use data from virtual locations
   - Less restrictions on data use for a variety of purposes that provide value
   - Less administrative overhead and less red tape

Camouflage

Complications of Data Masking

1. Data Utility - masked data must look and act like the real data
2. Data Relationships - must be maintained after masking
3. Existing Business Processes - needs to fit in with existing processes
4. Ease of Use - must balance ease of use with need to intelligently mask data
5. Customizable - must be able to be tailored to specific needs

Camouflage

Complications of Data Masking

1. Data Utility - masked data must look and act like the real data
   - proper testing and development
   - application edits
   - data validations
2. Data Relationships - must be maintained after masking
   - database level RI
   - application level RI
   - data synchronization (interrelated database RI)

Camouflage

Complications of Data Masking

3. Existing Business Processes - needs to fit in with existing processes
   - fit in with existing IT and refresh processes
   - automation of masking process
4. Ease of Use - must balance ease of use with need to intelligently mask data
   - need to have usable data that does not release sensitive information
   - knowledge of specialized IT/privacy topics and algorithmics should be pre-configured and built into masking process

Camouflage

Complications of Data Masking

5. Customizable - must be able to be tailored to specific needs
   - any solution/process must have the ability to be easily updated and customized
   - must have ability for masking methods and the overall solution to be customized

Camouflage

Product Requirements

- 4 Broad Categories of Evaluation
  1. Database Support
  2. Application Support
  3. Platform/System Support
  4. Functional Requirements

Specific Requirements

1. Built on Open Standards
   - ✓ Ensures a solution that is flexible and portable if IT requirements and strategies change
   - ✓ Database and platform independence - provides broad database and platform support
   - ✓ Provides a level of application independence, including custom applications
2. Multi-Database Connectivity
   - ✓ Required for integrated environments where several applications/databases interact

Specific Requirements

3. Support 3 Levels of Relational Integrity:
   - ✓ ***Database Defined:*** Easily references and relies on meta-data and ensures that all indexes, triggers, etc. are maintained
   - ✓ ***Application Defined:*** Simplifies the process of enforcing application-defined relationships – e.g. PeopleSoft
   - ✓ ***Data Synchronization:*** Ability to synchronize masked values across databases within integrated environments

Specific Requirements

4. Common Interface
   - ✓ Common interface and functionality available regardless of platform or database – avoid specialized versioning
   - ✓ Open standards provides this database and platform independence
5. Formal and Repeatable Methodology
   - ✓ Masking configuration process should be re-useable and repeatable while maintaining security of original data (randomization of masking methods required)
   - ✓ Configurations should be portable between databases and platforms

Camouflage

Specific Requirements

6. Variety of Delivered Masking Methods
   - ✓ Does solution come with a variety out-of-the box masking methods
   - ✓ Avoid having to build yourself
7. Customizable
   - ✓ ***Scripting Capability:*** Does solution have ability to create/define customized masking methods, and can they be used alone and in conjunction with delivered masking methods
   - ✓ Easily account for a variety of special organizational circumstances

Camouflage

Specific Requirements

8. Security and Utility of Masked Data
   - ✓ Are masking methods intelligent and robust
   - ✓ Is randomization of masking methods present, and does solution appropriately mask data (sufficiency, computationally correct, fully functional, etc.)
9. Ease of Use
   - ✓ Simple to install, intuitive and easy to use
   - ✓ No manual mapping from source to destination database(s), no manual mapping of relationships, etc.
   - ✓ Included as part of an automated refresh process

Camouflage

Specific Requirements

10. Automation
    - ✓ Included as part of an automated refresh process
    - ✓ Removes human element
    - ✓ Automatically account for database changes

Looking Ahead…

- Security experts predict:
  - security, privacy, and identity management will remain at the top of information security spending priorities
  - the incidence of data breaches will continue to rise unless organizations enforce additional measures to protect sensitive data; both in production and non-production environments

Comments & Discussion

Paul Preston
(613) 421-6332
ppreston@platogroup.com

National Privacy and Security Guidelines: A Canadian Experience in Jurisdiction-Wide Use
Elaine Sawatsky, Management Consultant, Privacy and Security

Abstact:
In this presentation Elaine will review the history of the COACH security and privacy guidelines, and provide an update on the changes in the 2006 revision and the reasons for these changes.

Bio:
Ms. Elaine Sawatsky is an information systems professional with extensive and up-to-date knowledge and experience specializing in Privacy and Security policies and programs. She has an in-depth understanding of the need for, and the implementation issues associated with, organizational Security and Privacy programs and practices. Her experience in program implementation and change management, as well as experience with organizations attempting to address security problems, coalesces in a business-driven, practical approach to data protection.

Ms. Sawatsky has gained an understanding of provincial and national health business environments through over 30 years experience dealing with a Provincial Health Ministry, with physicians, and in public and private health care institutions.

Public, Provider and Government

National Privacy and Security Guidelines

A Canadian Experience in Jurisdiction-Wide Use

COACH
Canada's Health Informatics Association

1

Coach – Canada's Health Informatics Association

Agenda

- About COACH
- Jurisdiction licensed use of Privacy and Security Guidelines
  - Challenges and issues in privacy and security of health information
  - The Guidelines !!
  - Guidelines use by Jurisdictions
  - Other applications / uses of the guidelines

2

Coach – Canada's Health Informatics Association

- COACH Vision:
  Taking Health Informatics Mainstream
- Members interested in advancing the practice of health informatics in Canada (multidisciplinary)
- Support for use of the Guidelines comes from the Jurisdictions themselves

3

Current state of Privacy and Security – for all of us

- In Canada and the EU, Privacy & Security Legislation is based on International Principles
- Privacy is a requirement for Canada's EHR
- Awareness raising needed to bring all healthcare providers to the same place
- Principles and requirements must be part of everyday business - consistent

4

Canadian directions for privacy and security

Similarities

- same foundation across Canada
- Same principles generally apply
- Principles are understood: ethics, human rights

Differences

- Jurisdictions have some differences
- Consent & Health Information Acts
- different process in different provinces

5

Privacy and security issues across Canadian Jurisdictions

- Differences in approach to consent
- Who should have access? Based on need-know. Easy to say/Hard to do
- How can specific access based on Need to Know be controlled?
- Secondary uses an issue
- Research issues and process unresolved in some provinces

6

Privacy and security jurisdiction strategies

- Ab: HIA & FOIPPA & PIPA & PIPEDA
- On: New HIA. Improved in some ways
- BC: no HIA all data protected similarly, but generally. Little specific Health advice
- BC new Health Act amendments - Effect is yet to be seen

7

The COACH Privacy and Security Guidelines

Process:

Improve Content

Increase Relevance

Describe Jurisdictional Differences of Legislation

Culture of Healthcare Information Sharing

Culture of Data Protection

8

Jurisdiction application of the guidelines

We are addressing:

General requirements in privacy and security

Provincial needs especially those of the licensees

AB and SK will have input into content

Support for Multiple Stakeholders

9

Jurisdiction application of the guidelines

Why Licensing?

- Resource for Alberta and Saskatchewan Ministries of Health
- Can be provided electronically and used in many communications channels.

10

Broad application of the guidelines

Adaptable:

Licensees can use the content electronically

Can have input into how the content is framed

Can add their jurisdictional 'messages'

11

2006 COACH Guidelines Revision

- Why Revise?
- What should be revised?
- How should it be managed? Undertaken?

12

2006 COACH Guidelines Revision

- Why
- Improve quality
  - Improve Format and Readability
  - Readiness for Licensing
  - Licensing provides revenue which can be spent on improved product, demands improved quality and drives on-going currency
  - Currency of content

13

2006 COACH Guidelines Revision

- What should be revised?
  - New format identifies weak areas
  - New format allows on-going currency
  - Weak areas to be improved

14

2006 COACH Guidelines Revision

- How?
  - Steering Committee: COACH, AB, SK
  - Expert Working Group – Chair, X-Canada experts
  - More hands-on from COACH
  - More reviews during the revision process

15

2006 COACH Guidelines Revision

- Content is the same whether paper or 'e'
- Content framed in a consistent manner for inter-provincial use.
- Current format was framed around an ACHI concept that is not widespread in use which makes it somewhat obscure and not translatable.
- The appropriate framework will make the content more recognizable and useful if a frame is chosen which is well known and broadly used.

16

2006 COACH Guidelines Revision

- **New Format/Framework**
- Align with the principles of the CSA Model.
- The ISO 17799 standard fits this frame as Security falls under Principle #7, Safeguards.
- Makes it applicable to both private and public sector
- Differences in provincial legislation can be noted under each heading
- Additional subject matter as per headings from the ISO 17799 Security Management Standard can be inserted

17

2006 COACH Guidelines Revision

- **Process**
- Began with an outline for the whole document
- Critique to Committee members and then SC, then External Reviewers
- Content from current guidelines inserted
- Content revised, reviewed as created and then as a complete document.
- External reviews at all steps of the process
- This time we will benefit from a macro external analysis to see where the change drivers are coming from

18

2006 COACH Guidelines Revision

EWG membership - Chair: Elaine Sawatsky

- Cindy Brice, Eric MacDonald, Patrick Lo, Guy Patterson, Marianna Catz, Jane Dargie, Jayden Stevens, Nikki Shaw.
- External Reviewers: Ross Fraser, Pat Jeselon, Andrew Hughes, Colin Booth, David Loukidelis, Ruth Yeo, Brendan Seaton, Pat Coward, Gerry Bliss, Pierrot Peledeau

19

2006 COACH Guidelines Revision

- More external reviewers are needed
- Volunteers are appreciated
- ?? Questions??

20

For Better, Not Worse: Data Protection and Health Research

Val Steeves, University of Ottawa

Abstract:
This presentation challenges the argument that data protection legislation may harm research by unduly restricting the flow of personal health information. I unpack the assumption that privacy is an individual right that must give way to research as a social good, and explore how data protection laws facilitate the flow of information for research purposes. I conclude that researchers should embrace data protection laws because they help to construct trust in research practices, mitigate the commercial imperatives which flow from the fact that research is a public-private enterprise, and protect the accuracy of data. And since research databases do not exist in isolation, researchers must respect the fact that the non-consensual flow of information poses risks of harm – including the secondary use of health research databases for social control – that must be managed.

Bio:
Valerie Steeves is an Assistant Professor in the Department of Criminology at the University of Ottawa. Her main area of research is the impact of new technologies on human rights issues. Professor Steeves is also an internationally recognized expert on privacy law, and is an active participant in the legislative and policy debate regarding the privacy of personal health information. In 2004, she was awarded McMaster University's LaBelle Lectureship for her work on health privacy. The LaBelle Lectureship is a juried prize that recognizes scholars doing cutting-edge interdisciplinary work and challenging accepted ideas. Professor Steeves was called to the Bar of Ontario in 1984 and practiced law in Toronto until she began teaching in 1990.

For Better, Not Worse: Data Protection and Health Research

Professor Valerie Steeves
Department of Criminology
University of Ottawa

"Privacy rules may threaten research: Following PIPEDA has led to biased data for Canadian Stroke Network"

- Medical Post
April 20, 2004

- Busby, A. et. al. (2005). Survey of informed consent for registration of congenital anomalies in Europe. British Medical Journal 331:140-141.
- Tu, J. et al. (2004). Impracticability of Informed Consent in the Registry of the Canadian Stroke Network. The New England Journal of Medicine. 350 (14): 1414 - 1422.
- Ingelfinger J. & J. Drazen. (2004). Editorial: Registry research and medical privacy. The New England Journal of Medicine 350(14): 1452-1453.

Misconception No. 1

Data protection laws restrict access to health information for research purposes.

Ontario Personal Health Information Protection Act, 2004

Section 44(1) Disclosure for research

A health information custodian ***may disclose personal health information*** about an individual ***to a researcher if the researcher submits*** to the custodian …***a research plan*** … and a copy of the decision of a research ethics board that approves the research plan.

Misconception No. 2

Research is an unencumbered public good free of any private interest.

- American Medical Association - $20 million (US) for doctors' biographies
- Big Pharmas - $12 billion (US) for direct marketing to physicians
- IMS - $1.3 billion (US) for health information

Misconception No. 3

Privacy is an individual right and so must give way to research as a public good.

- Most privacy scholars emphasize that the individual is better off if privacy exists. I am arguing that society is better off when privacy exists. I argue that society is better off because privacy serves common, public and collective purposes. If you could subtract the importance of privacy to one individual in one particular context, privacy would still be important because it serves other important functions beyond those to the particular individual

  - Priscilla Regan

Misconception No. 4

Observational research data collected without the patient's knowledge and consent will lead to unbiased data.

- Just under 10 percent feel that doctors will not use their personal health information (Mulligan, 2001).
- Over one-quarter of teens will not seek out health care if they are concerned about confidentiality (Cheng, et. al., 1993).

- One in ten people have changed their behaviour to protect their medical privacy by:
  - going to another doctor
  - paying direct
  - not seeking medical care
  - giving inaccurate or incomplete information
  - asking the doctor not to record
- People who know their medical privacy has been breached in the past are four times more likely to participate in these behaviours.
  (California Healthcare Foundation, 1999).

Misconception No. 5

Privacy is a road block to better health.

Privacy as a determinant of:

- Mental health (Goffman, 1996)
- Psychological health (Altman, 1975)
- Emotional health, suicide (Westin, 1967)
- Emotional, psychological and physical well-being (Woogara, 2001)

Misconception No. 6

Deidentified health information does not pose a risk of harm to the patient.

- [In a surveillance society] record linkages are so easy to accomplish that the power holders cannot resist using them to try to solve real and alleged social problems.

  - David Flaherty

- [Although organizations often use surveillance to] solve problems of genuine social importance … if all that has to be done to win legal and social approval for surveillance is to point to a social problem and show that surveillance would help cope with it, then there is … only a qualifying procedure for a licence to invade privacy.

  - Alan Westin

Realities about Privacy and Research

- Data protection laws are a useful tool for researchers because they help to construct trust in research practices.
- Rules and regulations regarding the flow of medical information are needed to mitigate the commercial imperatives which flow from the fact that research is a public-private enterprise.
- Privacy is a social value which must be built into good research design.

Realities about Privacy and Research

- Good privacy practices promote research because they protect the accuracy of data.
- Privacy is an essential element of psychological health and healthy social relationships.
- Research databases do not exist in isolation, and researchers must respect the fact that the non-consensual flow of information poses risks of harm.

vsteeves@uottawa.ca

Statistical Disclosure Control Techniques and Issues

Jean-Louis Tambay, Assistant Director, Household Survey Methods Division, Statistics Canada

Abstract:
The presentation gives an overview of statistical disclosure control techniques and issues as they relate to statistical organizations. The presentation starts with a few definitions of disclosure and an outline of characteristics affecting disclosure. Problems and approaches to disclosure control are then given in the context of tabular data, microdata and analytical outputs. The objective of the presentation is to provide a general understanding of the disclosure issues for different types of outputs and to learn about common approaches to the problem.

Bio:
Jean-Louis Tambay has a Bachelor's Degree in Mathematical Statistics from the University of Manitoba (1979) and a Masters Degree in Statistics from Carleton University (1985). He is an Assistant Director in Household Survey Methods Division at Statistics Canada, where he has worked for 27 years. He has been involved in statistical data confidentiality in the last ten years and had provided training, consultation as well as carried out research in the areas of protection of microdata and tabular data. He chairs the agency's Disclosure Control Resource Centre and Disclosure Review Committee, sits on the Confidentiality and Legislation Committee, Microdata Release Committee and Privacy Impact Assessment Review Group, and provides consultation on disclosure control to Statistics Canada's Research Data Centres.

Overview of Practices to De-identify Data Releases

Jean-Louis Tambay
Statistics Canada

Electronic Health Information & Privacy Conference
November 13, 2006

Objectives for the Presentation

- Identify types and causes of disclosure
- Understand the disclosure issues for different types of outputs
- Learn about common approaches to the problem
- Obtain references on the subject
- Get the opportunity to ask questions

2

Outline

- Overview
  - Definitions
  - Characteristics affecting disclosure
  - Approaches to disclosure control
- Tables of magnitude
- Frequency tables
- Analytical outputs
- Microdata
- Alternate access methods
- References

3

Confidentiality and Disclosure

- When data are released, we must protect the confidentiality of respondents' data and identity.
- Disclosure relates to the inappropriate attribution of information to a data subject, whether an individual or an organization.

4

Identity Disclosure

When an individual data subject (respondent) can be identified from the released data

- More of a problem with microdata outputs

Some causes of identification:

- Well-known personality or enterprise
- Self-disclosure (intentional or not)
- Successful attempt at disclosure (e.g., using record linkage)
- Spontaneous recognition

5

Attribute Disclosure

When confidential information is revealed and can be attributed to an individual

- Can occur with tabular outputs

Examples:

- « All persons with characteristic x have characteristic y »
- « People in occupation x make $ 50-60,000/year »
- « 99% of people with characteristic x have characteristic y »

6

Inferential (Probability) Disclosure

When information about an individual can be inferred with a high level of confidence (low level of uncertainty)

Although not normally an issue – making inferences is a major objective of statistical analysis – it could become one if we single out small & identifiable populations.

7

Residual Disclosure

When confidential information is disclosed by the combining of information.

Examples:

- Reconstitution of suppressed cells in tables
- Getting small area level information using data from overlapping geographical areas
- Combining released and publicly available information to reveal confidential data
- Exploiting relationships such as:

#RichNonWhites = #All – #NonRich – #Whites + #NonRichWhites

8

Sample Surveys *vs* Admin Data

Censuses and Administrative Data have higher disclosure risks than sample data:

- No uncertainty if a unique person is identified
- Little/no uncertainty under attribute disclosure

Sampling reduces disclosure risks:

- Uncertain that unique individuals in the sample are unique in the population (mistaken identity?)
- Attribute disclosure must allow for sampling error
- Sampling can be used as a disclosure control tool

9

Types of Outputs

By decreasing level of risk:

- Anonymized microdata at respondent level
  - Requires thorough checking for confidentiality
- Tables of magnitude data
  - Problem of dominance (especially Business data)
- Frequency tables
  - Possibility of attribute disclosure
- Analytical results (graphs, model outputs...)
  - Least risk – but disclosure can still occur

10

Approaches to Disclosure Control

- Restricted Access Methods
  - Access to buildings, passwords, encryption...
  - Research Data Centres, Remote Access, License Agreements, Data Sharing Agreements
- Restricted Data Methods
  - Data Reduction Methods
  - Data Perturbation Methods
- Other (waivers)

11

Outline

- Overview
- Tables of magnitude
- Frequency tables
- Analytical outputs
- Microdata
- Alternate access methods
- References

12

Tables of Magnitude

- Cells represent quantitative amounts
- More problematic for financial and business data – data distribution is often skewed with a few large values
- Disclosure may occur in two ways:
  - From the released data
  - After combining released data with other information

13

Tables of Magnitude

- Identify sensitive cells
  - Sensitivity due to dominance and small cells (less than *n* contributors)
- Determine method to protect them
- Common solutions:
  - cell suppression (& complementary suppression)
  - cell aggregation (collapse rows/columns)
  - addition of noise (to microdata or aggregates)

14

Example 1 of Cell Suppression

2	3	5
?	92	95
5	95	100

15

Example 1 of Cell Suppression

?	?	5
?	?	95
5	95	100

16

Example 1 of Cell Suppression

0-5	0-5	5
0-5	90-95	95
5	95	100

17

Example 2 of Cell Suppression

X	X	X	15	20
15	X	X	20	55
X	10	10	X	25
X	6	15	X	35
20	30	35	50	135

18

Example 2 of Cell Suppression

X	24		15	20
15			20	55
X	10	10	X	25
X	6	15	X	35
20	30	35	50	135

19

Example 2 of Cell Suppression

1	24		15	20
15			20	55
X	10	10	X	25
X	6	15	X	35
20	30	35	50	135

20

Outline

- Overview
- Tables of magnitude
- Frequency tables
- Analytical outputs
- Microdata
- Alternate access methods
- References

21

Frequency Tables

- Contents of cells represent numbers of units or weighted numbers of units (for survey data)
- Disclosure issues with frequency tables:
  - Zero cells and full cells
  - Small cells
  - Residual disclosure
- Disclosure is more of a problem with census or administrative data

22

Zero Cells and Full Cells

- Can lead to attribute disclosure if they reveal sensitive information
  - e.g., absence of a characteristic like “employed”
  - e.g., income distribution in a specific range
- Zero Cells have no respondents
  - a structural zero cell represents an invalid combination (e.g., “Married” & “Under 15”)
- Full Cells contain all the respondents from a marginal total
  - e.g., the only nonzero cell in a row or column

23

Zero Cells and Full Cells (cont.)

Income	Cat. A	Cat. B	Cat. C
<20K	0	7	0
20-40K	36	16	12
40-60K	23	0	45
60-80K	7	0	13
80-100K	0	5	1
Total	66	28	71

24

Small Cells

- Cells containing few observations (e.g., <3)
- May present a disclosure risk for census data
  - e.g., Teenagers in a particular CMA with AIDS: 2
    - disclosure risk if additional info is given about them
  - e.g., Companies in Industry A using technology X: 1
    - that company knows the competition does not
    - may confirm competition's suspicion it uses technology X
  - e.g., Cancer deaths in postal code area in 2002: 1
    - if only one death occurred in 2002 we revealed the cause
- Often gives the impression of a breach of confidentiality – even if none has occurred

25

Disclosure Control for Frequency Tables - Solutions

- Category regrouping (loss of information)
- Cell suppression (needs secondary suppression)
- Rounding (affects additivity in tables)
- Table restrictions (for query systems)
  - minimum area population size (e.g., 100 persons)
  - maximum number of variables (dimensions)
  - unacceptable combinations (e.g., geography & race)
  - minimum average &/or median cell size
- Perturbation of underlying data (introduces error)

26

Rounding

- Deterministic Rounding
  - e.g., round 10-14 down to 10; 15-19 up to 20
  - can give biased results
- Random Rounding

value	10	11	12	13	14	15	16	17	18	19	20
pr(=10)	1	.9	.8	.7	.6	.5	.4	.3	.2	.1	0
pr(=20)	0	.1	.2	.3	.4	.5	.6	.7	.8	.9	1

  - unbiased results, outcome not the same every time
- Controlled Rounding
  - preserves relationship between rounded values and rounded totals in a given table
  - not always possible for >2-dimensional tables

27

Residual Disclosure

- Occurs when tables are combined to reveal confidential data
- Geographical Data
  - large areas may overlap partially, leaving “slivers” with few units
  - “safe” areas may be subtracted from larger areas
- On-line query systems
  - related 2-dimensional tables can be combined to give ranges for cell values in higher dimensional tables
  - targeted attacks by hackers may be used to undo random rounding protection or circumvent table restriction measures

28

Outline

- Overview
- Tables of magnitude
- Frequency tables
- Analytical outputs
- Microdata
- Alternate access methods
- References

29

Analytical Outputs

- While analytical outputs are usually « safe » consider the following:
  - Graphs & scatterplots can display individual values
  - Minimums and maximums relate to individual values
  - Proportions of zero or one are like zero cells
  - Should minimum respondent rules in tables also apply to individual statistics such as means and variances?
  - Rules for individual statistics should also apply to statistics directly derived from them (e.g., ratios, covariances, correlations, $\beta_{HAT}=S_{xy}/S_x^2$)

30

Outline

- Overview
- Tables of magnitude
- Frequency tables
- Analytical outputs
- Microdata
- Alternate access methods
- References

31

Public Use Microdata Files

- Files of anonymised individual data from a sample of units created for research purposes
- Typically their release is subject to organisational guidelines and requires the approval of an Institutional Review Board
- Of particular interest is the protection from identification of persons with unique combinations of indirect identifiers
  (e.g., region, gender, age, marital status, race, occupation, chronic condition, household size, dwelling type, income level)

32

Disclosure Control for PUMFs

- Disclosure risk is higher with PUMFs:
  - they provide a rich data content
  - records can be compared against other databases in an attempt to identify unique matches
  - respondents can self-identify (& find others)
  - risks depend on population characteristics, geographical & other detail, sampling rate, etc.
- A main concern is with population uniques that fall in the sample – in survey samples we do not know who these units are

33

Disclosure Control Strategies

- Idea is to reduce number of sample uniques and/or introduce uncertainty in the data
- Methods can be applied globally or locally
- Data Reduction Methods
  - suppress/recode variables, use top-coding
  - suppress individual records (sample) or values
  - use microaggregation
- Data Perturbation Methods
  - swap data between records
  - impute data, round values, add noise to data

34

Outline

- Overview
- Tables of magnitude
- Frequency tables
- Analytical outputs
- Microdata
- Alternate access methods
- References

35

Alternate Access Methods

- Why?
  - PUMFs & custom tabulations cannot satisfy many researchers
  - Too much information is suppressed in ensuring confidentiality of PUMFs
  - Few longitudinal PUMFs were released
- Examples of alternate access methods:
  - Restricted access to microdata using data centres
  - Remote access/on-line query systems
  - Limited access to data under a license agreement

36

Research Data Centres

- Provide access to confidential data in a secure STC environment in universities
- For researchers with approved projects sworn-in as deemed employees under the *Statistics Act*
- Always staffed by STC analyst who vets outputs to be taken out for confidentiality
- Mostly longitudinal & household survey data

37

Remote Access

- Provides indirect access to survey data without compromising confidentiality
- Approved researchers obtain survey documentation and dummy (test) files
- They e-mail analytical programs to STC
- Programs are run on microdata at STC
- Outputs are vetted for confidentiality before being e-mailed back to researchers

38

Query Systems (American FactFinder)

- Internet access to 2000 Census data
- Recoding and swapping of underlying data
- Query & Results Filters:
  - restrictions on geogr. areas & cross-tab. vbles.
  - restrictions on combinations of variables
  - max. 3 variables, excluding geography
  - selected measures (means, medians, …)
  - time/size limits on requests
  - minimum mean & median cell sizes
  - limit on ratio of cells of size one

39

References (1/2)

- Federal Committee on Statistical Methodology. (2005). Report on Statistical Limitation Methodology. Statistical Policy Working Paper 22 – Second version, Office of Management and Budget, Washington, D.C. (http://www.fcsm.gov/committees/cdac/cdac.html/)
- Interagency Confidentiality & Data Access Group. (1999). Checklist on Disclosure Potential of Proposed Data Releases, Office of Management and Budget. (Same site as WP22).
- Jabine, T.B. (1993). Statistical Disclosure Limitation Practices of United States Statistical Agencies. Journal of Official Statistics, Vol. 9, No. 2. (www.jos.nu).

References (2/2)

- Expanding Access to Research Data: Reconciling Risks and Opportunities (2005) (http://www.nap.edu/catalog/11434.html)
- Improving Access to and Confidentiality of Research Data: Report of a Workshop (2000) (http://books.nap.edu/books/0309071801/html/index.html)
- For the Record: Protecting Electronic Health Information (1997) (http://books.nap.edu/books/0309056977/html/index.html)
- Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics (1993) (http://books.nap.edu/books/0309047439/html/index.html)

41

Concluding Thoughts

- Disclosure control is very complex and subjective
- Solutions are trade-offs between availability of data (quality to analysts) and protection of confidentiality
- It is impossible to guarantee absolute confidentiality

42

Living the nightmare: notifying affected persons after a privacy breach

Catherine Tully, Senior Portfolio Officer, Office of the Information & Privacy Commissioner, British Columbia

Abstract:
Your laptop or deskop computer is stolen. It's not difficult to replace. But what if it contains a database of sensitive personal information? What do you do if the information isn't just tombstone data, but also transcripts of intensely personal counseling sessions? What do you do if the data subjects represent a spectrum of psychological vulnerabilities, and you cannot predict their reactions to the notification process? Do you notify or not? What if there is no research data to assist you in designing a notification process that will address these unknowns? How do you proceed?

Bio:
Catherine is currently a Senior Portfolio Office at Office of the Information and Privacy Commissioner of British Columbia responsible for policy development, mediations and investigations, with 8 years as a staff lawyer in the Ontario Legal Clinic System, 2 years as an anti-poverty advocate for the Together Against Poverty Society (Victoria), and 5 years as the Director of the Privacy, Information and Records Management Division for the Ministry of Attorney General of British Columbia. She has a bachelor and law degree from the University of Ottawa and a Masters in law from Dalhousie University – International Law and Human Rights. She is also author of “Public Reporting of Child Death Reviews, April 2006”, B.C. Child & Youth Review (available at:
http://www.childyouthreview.ca/down/Public_Reporting_of_Child_Death_Reviews.pdf)

Notifying Affected Persons After a Privacy Breach

Catherine Tully
Office of the Information & Privacy Commissioner
British Columbia

Introduction

- What is a privacy breach?
- Four key steps when responding to privacy breaches
- Privacy breach notification
  - Is notification required?
  - How & when to notify
  - What to include in a notification

What is a privacy breach?

- Broad approach in British Columbia:

A privacy breach occurs when there is unauthorized collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the Personal Information Protection Act or part 3 of the Freedom of Information and Protection of Privacy Act.

4 Key Steps

Step 1: Contain The Breach

Step 2: Evaluate the risks associated with the breach

Step 3: Notification

Step 4: Prevention

Assessment Tools

- Privacy Breach Reporting Form
  (available at: http://www.oipcbc.org/forms/PrivacyBreachForm(Nov2006).pdf)
- Notification Assessment Tool
  (coming soon to BC OIPC & Ontario IPC)

Privacy Breach Reporting Form

- Purpose of the form:
  - Record essential facts – walks user through the 4 key steps including decisions regarding whether or not to notify
  - Send to privacy commissioner where required

Notification Assessment Tool

Answers three questions:

1. Is Notification Required? (Whether & Whom to Notify)
2. How and When to Notify
3. What to Include in a Notification

Privacy Breach Scenario

- Break in at a counselling centre
- Hard drive used as a server is stolen
- Hard drive holds name, address, S.I.N., personal health number, diagnosis, treatment plan & counsellor's notes of 8,000 current & former employees
- Password protected, no encryption

Why Notify?

- The main purpose of notification is to allow individuals or groups to avoid or mitigate harm resulting from the privacy breach.

Is Notification Required?

- In some jurisdictions (including Ontario), notification is required.
- Ontario:
  - Section 12(2) of PHIPA requires a health information custodian to notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.

Is Notification Required?

- In the United States:
  - 32 states have notice of security breach laws
  - Variety of tests but usually notification is required if there is a reasonable likelihood of harm to consumers
  - 30 states specifically exempt organizations from notifying where the lost information is encrypted

Is Notification Required?

- How do you decide whether and whom to notify?

Is Notification Required?

- Evaluate the risks to determine whether notification is required.

Is Notification Required?

Risk	Whom to Notify
Identity Theft Loss of SIN, credit card #, dl #, phn, debit card with password	•Individuals affected •Consumer reporting agencies •Police •Issuing authority

Is Notification Required?

Risk	Whom to Notify
Risk of Physical Harm When the loss of information places any individual at risk of physical harm, stalking or harassment	•Individuals affected •Police

Is Notification Required?

Risk	Whom to Notify
Hurt, humiliation, damage to reputation Associated with loss of information such as mental health records, medical records, disciplinary records	•Individuals affected •Treating health care professional

Is Notification Required?

Risk	Whom to Notify
Breach of contractual obligations Contractual provisions may require notification of third parties in the case of a data loss or privacy breach	•As per contractual provisions

Is Notification Required?

Risk	Whom to Notify
Future breaches due to similar technical failures Notification may be necessary if a recall is warranted and/or to prevent future a breach by other users	•Supplier of technology •Colleagues using the same technology

Is Notification Required?

Risk	Whom to Notify
Failure to meet professional standards or certification standards	•Professional regulatory body •Certification authority

Notification of the Privacy Commissioner

- ✓ There is a statutory obligation to report
- ✓ If no statutory obligation to report consider:
  - ✓ The information could be used to commit identity theft
  - ✓ Sensitive personal information is at risk
  - ✓ There is a reasonable possibility of harm including non pecuniary losses
  - ✓ The information has not been fully recovered
  - ✓ There is an ongoing threat of further disclosure or of unauthorized use of the personal information

Case Study: Is Notification Required?

- Counselling Centre hard drive holds unencrypted name, address, S.I.N., personal health number, diagnosis, treatment plan & counsellor's notes of 8,000 current and former employees

Case Study: Is Notification Required?

- ✓Risk of identity theft
- ✓Risk of hurt, humiliation, damage to reputation
- ✓Failure to meet professional standards?

- ✓Notification is required

Case Study: Who Must be Notified?

- ✓Individuals affected
- ✓Police
- ✓Consumer reporting agencies
- ✓Ministry of Health (to re-issue health card)
- ✓Treating health care professional
- ✓Professional regulatory bodies

When to Notify

When:

- Since the purpose of notification of individuals is to allow individuals or groups to avoid or mitigate harm resulting from the privacy breach, notification should occur **as soon as possible following the breach.**

When to Notify cont'd

- If the police have been notified, they may request that you delay notice in order to not interfere with their investigation

How to Notify

- Directly to the individual affected is preferred
- Multiple methods may be appropriate
- Determine first whether direct or indirect notification is appropriate
- Determine what method of notification will be most effective

Factors Favouring Direct Notification

- Personal information includes information that could be used for identity theft or involves medical information
- An identifiable group is affected and current contact information is available
- There is a risk of ongoing harm to individuals from the breach

Factors Favouring Direct Notification

- Individuals affected by the breach require detailed information in order to properly prevent harm or mitigate harm from the breach
- The security standard in applicable privacy legislation requires direct notification in the circumstances

Factors Favouring Indirect Notification

- Direct notification may result in a further breach of privacy and notice can effectively be given indirectly
- A very large number of individuals are affected by the breach and the likelihood of the harm occurring is low
- There are no mitigation steps possible for individuals affected by the breach such that the purpose of the notification would be for information only

Case Study: Direct or Indirect Notification

- Factors favouring direct notification
  - ☛Information could be used for identity theft
  - ☛There is a risk of ongoing harm
  - ☛Individuals require information to mitigate the harm from the breach

Case Study: Direct or Indirect Notification

- Factors favouring indirect notification
  - ☛Direct notification might cause emotional harm
  - ☛Direct notification could disclose the fact of psychiatric treatment to other family members
  - ☛Indirect notification could effectively provide the necessary information to affected individuals

Case Study: Direct or Indirect Notification

- ✓Indirect notification permitted
- ✓Counselling centre had access to employer's employee group e-mail list
- ✓Group e-mail effectively protected the identity of the subgroup of employees using the counselling centre services
- ✓Further information posted on the website

Methods of Notification

- Direct
  - Phone calls
  - Letters
  - In person
- Indirect
  - Through treating physician
  - Group email, electronic bulletin board
  - media

What to Include in Notification

- Description of the breach
- Description of the personal information inappropriately collected, used or disclosed
- Steps taken so far to mitigate the harm

What to Include in Notification

- Steps the individual can take
- Future plans for mitigation and prevention
- Contact information
- Right to complain to the privacy commissioner

Conclusion

- Notification is a key element of breach mitigation strategy
- If in doubt, notify
- Speed is essential - act quickly both to contain the breach and to notify

Conclusion cont'd

- Coming soon
  Breach Notification Assessment Tool
- British Columbia Information & Privacy Commissioner: http://www.oipcbc.org/
- Ontario Information & Privacy Commissioner: http://www.ipc.on.ca/