

# 2007 Electronic Health Information & Privacy Conference

December 3, 2007 – Ottawa, Canada

## Gold Sponsors



**Microsoft®**

## Silver Sponsor



**WINMAGIC®**  
**DATA SECURITY**

Knowing You're Protected

## Supporting Organizations

**CHITTA**  
HEALTH DIVISION OF ITAC / DIVISION DE LA SANTÉ DE L'ACTI

ASSOCIATION CANADIENNE  
D'INFORMATIQUE DE LA SANTÉ

**COACH**  
CANADA'S HEALTH  
INFORMATICS ASSOCIATION



## **PROGRAM**

### **REGISTRATION & WELCOME**

#### **OPENING STATEMENTS**

##### A Behavioral Perspective on Privacy Attitudes

Alessandro Acquisti

##### SSHA – A Renewal Story

Michael Power

### **BREAK**

#### **TRACK A**

##### **SESSION 1A: De-identification Techniques**

Chaired by Khaled El Emam,  
CHEO RI and University of Ottawa

##### **Presenters:**

Brad Malin,  
Vanderbilt University, USA  
Khaled El Emam,  
CHEO RI and University of Ottawa

#### **TRACK B**

##### **PANEL 1B: Global Information Flows**

Chaired by Anita Fineberg

##### **Panelists**

Adam Kardash,  
Partner, Heenan Blaikie  
Miyo Yamashita,  
President, Anzen Consulting Inc.

### **LUNCH**

##### **SESSION 2A: Medical Identity Theft**

Chaired by Gordon Atherley,  
Principal, Greyhead Associates

##### **Presenters:**

Jeff Curtis,  
Sunnybrook Health Sciences Centre  
Neil Stuart ,  
Partner, IBM Global Business Services

##### **SESSION 2B: Who's Responsible? Governance and the EHR**

Chaired by Joan Roch,  
Chief Privacy Strategist, Canada Health Infoway

##### **Presenters:**

Mary Lysyk,  
Policy Advisor, Health Canada  
John Cheung,  
Executive Director; eHealth Privacy,  
Security and Legislation, Knowledge  
Management and Technology Division,  
BC Ministry of Health  
Bill Trott,  
Director, Intergration for eHealth Privacy  
and Legislation, BC Ministry of Health  
Lucy MacDonald,  
Director of Privacy, Newfoundland and  
Labrador Centre for Health Information

**BREAK**

**PANEL 3A: Emerging Healthcare  
Technologies and the Future of  
Privacy**

Chaired by Ian Kerr,  
University of Ottawa

**Panelists:**

Jen Chandler,  
University of Ottawa

Vanessa Gruben,  
University of Ottawa

**SESSION 3B: Current Privacy  
Concerns and Proposed Design  
Recommendations**

Chaired by Mike Gurski,  
Director, Privacy Centre of Excellence,  
Bell Information and Communication  
Technology Solutions, Inc.

**Presenters:**

Bill Pascal,  
Chief Technology Officer, Canadian  
Medical Association  
Pierrot Peladeau,  
Centre for Bioethics, Clinical Research  
Institute of Montreal  
Patricia Kosseim,  
General Counsel, Office of the Privacy  
Commissioner of Canada  
Megan Bradley,  
Legal Counsel, Office of the Privacy  
Commissioner of Canada

**CLOSING REMARKS**

# Table of Contents

<b>Introduction</b>	<b>1</b>
<b>Opening Keynotes</b>	
<b>A Behavioural Perspective A Behavioral Perspective on Privacy Attitudes</b>	<b>2 - 35</b>
Alessandro Acquisti	
<b>SSHA – A Renewal Story</b>	<b>36 - 48</b>
Michael Power	
<b>Session 1A: De-identification Techniques</b>	<b>49</b>
Session Chair Khaled El Emam	
<b>Patient Re-identification and Anonymity Protection in Clinical Genomics Research</b>	<b>50 - 71</b>
Brad Malin	
<b>De-identifying Data for Health Research and Surveillance</b>	<b>72 - 90</b>
Khaled El Emam	
<b>Panel 1B: Global Information Flows</b>	<b>91</b>
Session Chair Anita Fineberg	
<b>Biography of Panelist</b>	<b>92</b>
Adam Kardash	
<b>Biography of Panelist</b>	<b>93</b>
Miyo Yamashita	
<b>Session 2A: Medical Identity Theft</b>	<b>94 - 106</b>
Session Chair Gordon Atherley	
<b>Identity Management in Healthcare</b>	<b>107 - 120</b>
Jeff Curtis	
<b>Medical Identity Theft</b>	<b>121 - 134</b>
Neil Stuart	

**Session 2B: Who's Responsible? Governance and the iEHR** 135 - 146

Session Chair Joan Roch

**Electronic Health Information and Privacy Survey: What Canadians Think – 2007** 147 - 163

Mary Lysyk

**eHealth in BC: A Work in Progress** 164 - 176

John Cheung & Bill Trott

**Session 3A: Emerging Healthcare Technologies and the Future of Privacy** 177

Session Chair Ian Kerr

**Negligence Liability for Breaches of Data Security** 178 - 188

Jen Chandler

**Privacy & Assisted Human Reproduction** 189 - 194

Vanessa Gruben

**Plenty of Eyes at the Bottom? nanomedicine and the future of privacy** 195 - 226

Ian Kerr

**Session 3B: Current Privacy Concerns and Proposed Design Recommendations** 227 - 232

Session Chair Mike Gurski

**A Pragmatic Look at Privacy, Medical Practice and the EHR** 233 - 238

Bill Pascal

**Designing Personal Information Networked Landscapes: Mirages, Quicksands and Safe Information Flow Paths Finding (English Version)** 239 - 245

Pierrot Peladeau

**Design des espaces d'informations personnelles réseautées : Mirages, sables mouvants et trajets sûrs pour flux d'informations (Version Français)** 246 - 251

Pierrot Peladeau

**So Who Wants to Know? Research Access to E.H.R. Data** 252 - 258

Patricia Kosseim & Megan Bradley

# **Introduction**

## **Electronic Health and Information Privacy Conference**

Recent high-profile security breaches make clear the importance of taking steps to protect sensitive personal information. For example, a memory stick containing personal information belonging to more than 500 Alberta pupils was stolen earlier this month. In January, a laptop containing health information of nearly 3,000 patients at Toronto's Hospital for Sick Children was stolen. Earlier this year, TJX, the parent company of Winners and HomeSense retail stores, announced that hackers had stolen data belonging to tens of millions of customers while CIBC's Talvest Mutual Funds lost data belonging to hundreds of thousands of customers. In fact, a random scan of media reports on any single day will find multiple stories of personal data being lost by or stolen from corporations and governments (see <http://ehip.blogs.com/ehip/> for an on-going tally).

There are potentially severe financial consequences to corporations who lose or expose personal data of their clients and users. For example, corporations suffer a non-trivial loss in their share price after the announcement of a security breach, with greater losses when the breach involves unauthorized access to confidential data. There is also the added effect of individuals losing trust in organizations that collect data from them. This results in decreased loyalty and higher churn among the customer base.

In addition to the negative impact on the data custodians, changes in the public's behavior to address perceived privacy risks can be detrimental to their well-being. In healthcare, concern about privacy has caused some members of the public to not be totally honest with their health care provider, go to another doctor, pay out-of-pocket when insured to avoid disclosure, not seek care to avoid disclosure to an employer, give inaccurate or incomplete information on medical history, and ask a doctor not to write down the health problem or record a less serious or embarrassing condition. Privacy concerns can hamper the effective adoption of electronic health records if not properly addressed and incorporated into their design.

This year's Electronic Health Information and Privacy conference continues to address contemporary privacy concerns with the adoption of information technology in health care and health research. We had speakers from across Canada and the US with research results and practical experiences dealing with privacy issues.

This volume contains the presentations and some of the notes from the conference.

**Khaled El Emam**

**Conference Chair**

# Opening Keynote

## A Behavioral Perspective on Privacy Attitudes

**Alessandro Acquisti, Carnegie Mellon University**

### **Abstract:**

The explicit application of economic reasoning to the study of privacy-related trade-offs started in the late 1970s, progressed in the 1990s, and flourished in the early 2000s with a number of formal micro-economic models and empirical studies. Such more recent studies have uncovered apparent inconsistencies and paradoxes in the ways individuals perceive, talk about, and act upon privacy needs. In particular, a dichotomy between individual stated privacy attitudes and actual behavior has been highlighted: individuals often claim to be highly concerned about their personal privacy, but few adopt technologies to protect it, and many release personal information in exchange for small rewards. Acquisti will present an overview of the economics of privacy and its behavioral paradoxes, and show how we can apply lessons from behavioral economics to understand individual privacy decision making. Finally, he will present results from some recent studies which test individuals' willingness to disclose private information about their health, finances, and sexuality as a function of different conditions: the paradoxical effects of reassurance on people's propensity to disclose private information; the impact of overt versus covert inquiries about sensitive behaviors; and the effect on peoples' willingness to disclose sensitive information of the order in which questions of varying degrees of sensitivity are asked.

### **Bio:**

Alessandro Acquisti is an Assistant Professor of Information Technology and Public Policy at the H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, and a member of Carnegie Mellon Cylab. His work investigates the economic and social impact of IT, and in particular the interaction and interconnection of human and artificial agents in highly networked information economies. His current research focuses primarily on the economics of privacy and information security, but also on the economics of computers and AI, agents and computational economics, ecommerce, cryptography, anonymity, and electronic voting. His research in these areas has been disseminated through journals (including Marketing Science, IEEE Security & Privacy, and Rivista di Politica Economica); edited books ("Digital Privacy: Theory, Technologies, and Practices." Auerbach, 2007); book chapters; and leading international conferences.

Prior to joining CMU Faculty, Acquisti researched at the Xerox PARC labs in Palo Alto, CA, and for two years at RIACS, NASA Ames Research Center, in Mountain View, CA. At RIACS, he worked on agent-based simulations of human-robot interaction onboard the International Space Station.

In 2000 he co-founded PGuardian Technologies, Inc., a provider of Internet security and privacy services, for which he designed two currently pending patents.

Acquisti has received national and international awards, including the 2005 PET Award for Outstanding Research in Privacy Enhancing Technologies and the 2005 IBM Best Academic Privacy Faculty Award. He is and has been member of the program committees of various international conferences and workshops, including ACM EC, PET, WEIS, ETRICS, WPES, LOCA, QoP, and the Ubicomp Privacy Workshop at Ubicomp. In 2007, he chaired the DIMACS Workshop on Information Security Economics and the WEIS Workshop on the Economics of Information Security. In the past, he has been a Research Fellow at the Institute for the Study of Labor (IZA) in Bonn, Germany.

In a previous life, Acquisti worked as classical music producer and label manager (PPMusic.com), arranger, lyrics writer (BMG Ariola/Universal), and soundtrack composer for theatre, television (RAI National Television), and indie cinema productions. He has lived and studied in Rome (Laurea, Economics, University of Rome), Dublin (M.Litt., Economics, Trinity College), London (M.Sc., Econometrics and Mathematical Economics, LSE), and a Ph.D. in Information Management and Systems from the University of California at Berkeley.

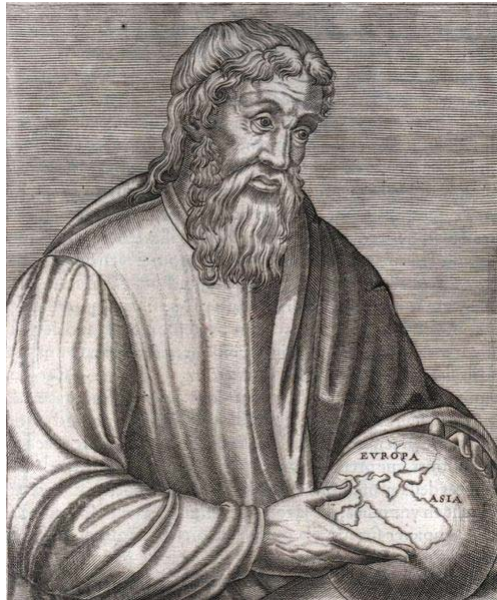
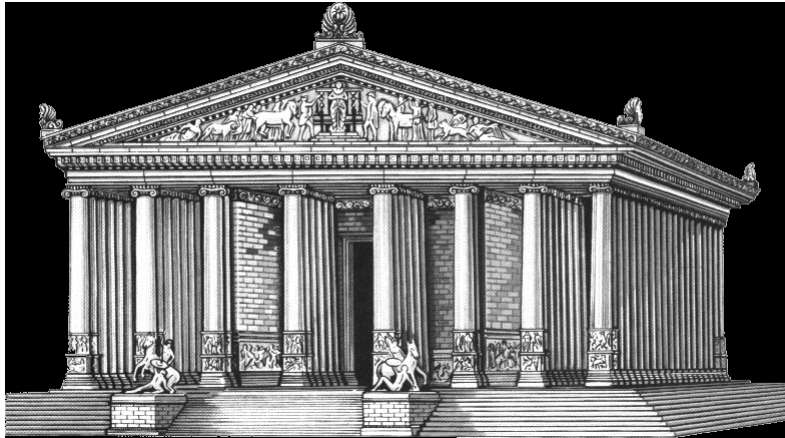


***Searching for Privacy  
in All the Wrong Places?  
A Behavioral Economics Perspective  
on Individual Concerns for Privacy***

Alessandro Acquisti  
Heinz School & CyLab  
Carnegie Mellon University

***EHIP Conference, December 3, 2007***







## Facebook's Group: "30 Reasons Girls Should Call It a Night"

From Salon.com

*"In one photo, a young woman is shown passed out in a bathtub, her miniskirt falling aside to reveal her underwear. Today she posted to the group's message board, "haha ... never expected to be in a UK newspaper when i posted pics here" and then a few minutes later, "almost famous I guess."*

# Agenda

---

1. From the economics of privacy...
  - Why privacy and economics
  - The paradox of privacy attitudes vs. privacy behavior
2. ... to the behavioral economics of privacy
  - Overview
  - Four recent studies (joint work with Leslie John and George Loewenstein)

---

The economics of privacy

## Privacy and Economics

---

- Privacy is an economic problem...
- ... even when privacy issues may not have direct economic interpretation
- Privacy is about trade-offs: pros/cons of revealing/accessing personal information
  - Individuals
  - Organizations
- ... and trade-offs are the realm of economics

## The Evolution of the Economics of Privacy

---

- Early 1980s
  - Chicago school
- Mid 1990s
  - IT explosion: Varian, Noam, Laudon, ...
- After 2001
  - **Microeconomic models**
  - Empirical studies
  - **Behavioral approaches**

## Privacy Attitudes...

---

- Attitudes: Usage
  - Privacy top reason for not going online (Harris Interactive in 2001)
  - 78% would increase Internet usage given more privacy (Harris Interactive)
- Attitudes: Shopping
  - \$18 billion in lost e-tail sales (Jupiter Research)
  - 73% would shop more online with guarantee for privacy (Harris Interactive)
- Attitudes: Experiments
  - Hann, Hui, Lee, and Png (2002): protection against errors, improper access, secondary use worth \$30.49 – 44.62 to American users
- Attitudes: Surveys
  - Alan Westin's clusters: pragmatists, unconcerned, fundamentalists

## ... versus Privacy Behavior

---

- Behavior
  - Anecdotal evidence

*"Ask 100 people if they care about privacy and 85 will say yes. Ask those same 100 people if they'll give you a DNA sample just to get a free Big Mac, and 85 will say yes."* Austin Hill
  - Experiments
    - Spiekermann, Grossklags, and Berendt (2001): privacy fundamentalists ♥ electronic cameras
    - Acquisti and Gross (2006): Facebook inconsistencies

## Facebook Inconsistencies

- Acquisti and Gross (2006): Little relation (insignificant Pearson *chi2* tests) between reported privacy attitudes and likelihood of providing certain information
- For instance:
  - 16% of respondents with highest concern in the “stranger knows your address and schedule” scenario provided that information
  - 16% of respondents with highest concern for “5 year scenario from now somebody will know your current political and sexual orientation, and your partners name” scenario provided all three types of information

## Reasons? Many

### Free Giveaway!

Name: \_\_\_\_\_  
Address: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Home Phone: \_\_\_\_\_  
Work Phone: \_\_\_\_\_  
☐ Single ☐ Married  
Age: \_\_\_\_\_ Occupation: \_\_\_\_\_  
Spouses Age: \_\_\_\_\_ Occupation: \_\_\_\_\_  
Combined Income:  
☐ Under \$30,000 ☐ Over \$30,000 ☐ Over \$50,000  
DO YOU: ☐ RENT OR ☐ OWN YOUR HOME?  
☐ VISA ☐ MASTERCARD ☐ AMERICAN EXPRESS  
Would you like info on special events & promotions at Pier 39?  
☐ Yes ☐ No  
E-mail address: \_\_\_\_\_

### Details of Participation and Eligibility Requirements

- Only one Entry per Family.
- Winner allows the use of his or her name, photo, and statements for future promotional use without further compensation.
- Winner must be 18 or over. I.D. required. Winner must provide all necessary federal and state tax reporting information before receiving prizes.
- Drawing held February 23, 2003. Last date to enter drawing is February 16, 2003.
- Winner need not be present to win. Winner will be notified by phone.
- Drawing will be conducted by a Certified Public Accounting Firm at the corporate office of Grand Pacific Resorts, 5900 Pasteur Ct., #200, Carlsbad, CA 92008. To request winner information, correspondence may be forwarded to Grand Pacific Resorts, Promotions Dept., P.O. Box 4068, Carlsbad, CA 92018.
- All local, state, and federal taxes, fees and licenses are the winner's responsibility. Acceptance of the prizes constitutes a release of Facility Management's agents and employees from all responsibility to the winner.
- Odds are based on number of entries received, approximately 1 in 700,000.
- No purchase or attendance is necessary to be entered into the drawing. Entrants may be invited to attend a sales presentation about the Red Wolf Lodge at Squaw Valley.
- Entries become the property of PNR Marketing Inc.
- The annual "Grand Prize" Giveaway consists of any vehicle with a retail value not to exceed \$25,000 or a three year lease (value to \$25,000) on a luxury car; or any prize (or similar) displayed in a Grand Pacific Resorts Promotion February 25, 2002 - February 23, 2003 (valued up to \$15,000), or the winner may choose cash in the amount of \$15,000.

## (Neo)classical Model of Privacy

---



Should I mention  
my sexual  
preferences on  
Facebook?

## (Neo)classical Model of Privacy

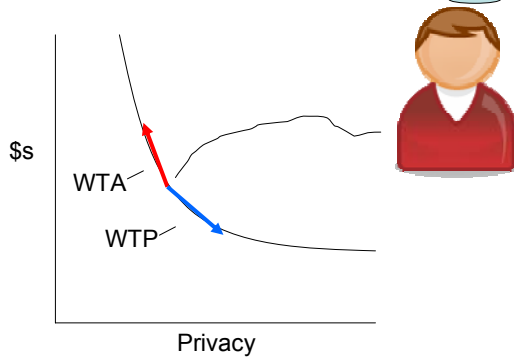


Maybe I'll find a lover... But what about my future job  
prospects? And what if my parents happen to log on...



## (Neo)classical Model of Privacy

$$\sum p_i \sum \frac{1}{(1+d)^t} u(\text{benefits}_{it}) - \sum q_i \sum \frac{1}{(1+d)^t} u(\text{costs}_{it})$$



## Why is this Problematic?

- Incomplete information
- Bounded rationality
- Psychological/behavioral distortions
  - Hence, behavioral economics

---

## The behavioral economics of privacy

## Behavioral Economics

---

- **Behavioral economics** combines psychology and economics
- Behavioral economics has studied several “deviations” from the theoretical rational behavior of the economic agent
- Many of those deviations have applications to the privacy arena...

## Possible applications of a “behavioral economics of privacy”

- Optimism bias...
- Complacency towards large risks...
- Inability to deal with prolonged accumulation of small risks...
- Time discounting...
  - E.g. O'Donoghue & Rabin, 1999; Frederick, Loewenstein, & O'Donoghue, 2002
- Adaptation and loss aversion...
  - E.g. Tversky & Kahneman, 1991; Frederick & Loewenstein, 1999
- Preference uncertainty & constructed preferences (coherent arbitrariness)...
  - E.g. Ariely, Loewenstein, & Prelec, 2003; Tversky, Slovic, & Kahneman, 1990)

## Four recent studies

1. The paradox of assurance
  2. Over vs. covert inquiries
  3. Coherent arbitrariness
  4. Willingness to pay vs. willingness to accept
- Joint work with Leslie John and George Loewenstein

# Study 1: The Paradox of Assurance

---

- Thesis
  - If people don't naturally think about privacy... then assurances can decrease divulgence
- Design
  - Paper and pencil survey
  - Respondents asked for email, then 12 questions
  - 3 condition between-subjects design
    - No assurance, weak assurance, strong assurance

## Weak and Strong Assurances

---

- Weak assurance

*"A quick note to let you know that any identifying information you may choose to provide in this survey will be stored separately from your responses. In addition, your survey responses will only be analyzed in aggregate."*
- Strong assurance

*"Concerning the confidentiality and anonymity of your responses: Please be advised that maintaining the confidentiality and anonymity of your responses is of the utmost importance to us. The following procedure will be used to maintain your anonymity in analysis, publication, and presentation of any results. Anonymity will be maintained during data analysis and publication/presentation of results by any or all of the following means: (1) You will be assigned a number as names will not be recorded. (2) The researchers will save the data file by your number, not by name. (3) Only members of the research group will view collected data in detail. (4) Any recordings or files will be stored in a secured location accessed only by authorized researchers."*

Please answer the following questions, which refer to your educational experience **since high school**.

	Yes	No
1. Since high school, have you ever handed an assignment in late?		
2. Are you currently taking at least four courses?		
3. Have you ever plagiarized text for any kind of assignment?		
4. Have you ever let a classmate copy from you during an exam?		
5. Do you arrive late to class more often than the majority of your classmates?		
6. On average, do you find the number of students in your classes to be conducive to learning?		
7. Have you ever copied a classmate's homework?		
8. Have you ever cheated on an exam?		
9. Have you ever requested an extension for an assignment?		
10. Do you regularly attend classes?		
11. Have you ever lied to a teacher in order to avoid taking an exam or handing in a term paper on time?		
12. Have you ever lied about your grade point average?		

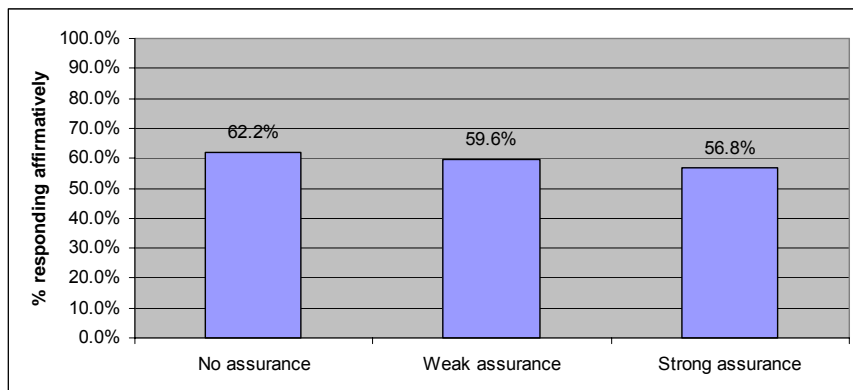
## Hypothesis

- Disclosure rates will be lowest in the strong assurance condition, but only for the sensitive items.

## Results

1. 95% (75/79) of participants gave us their .edu email address
2. Small reassurance had little effect, but substantive reassurance backfired (as predicted)

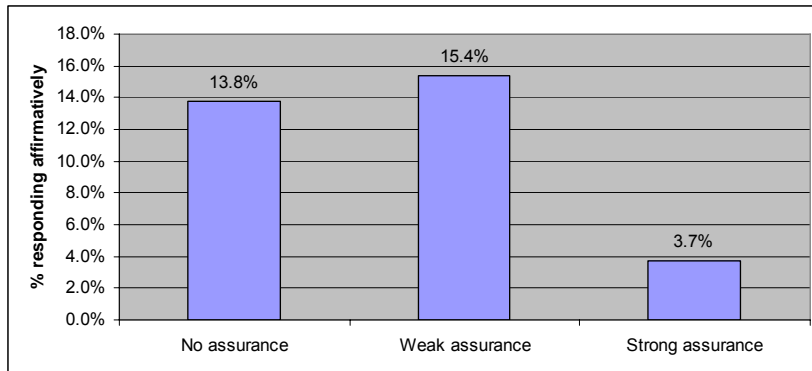
## Results: Innocuous Questions (6)



**N = 79**

**F(2,76) = 0.64, not significant**

## Results: Sensitive Questions (6)



**N = 82**

**$F(2,79) = 5.60, p = 0.005$**

## Study 2: Overt/Covert Inquiries

- Online survey posted on New York Times site
- All subjects asked for identifying information (email address)
- 34 questions pertaining to health, sex, and finances, ranging in intrusiveness
- 3 condition between subjects design

## Three Conditions

---

- **Point blank:** simply asks respondents whether they have engaged in 34 different behaviors, ranging from very mild to very intrusive
- **Commission:** rate how unethical the 34 activities are, but *only if you have engaged in them*
- **Omission:** rate how unethical the 34 activities are, but *only if you have not engaged in them*

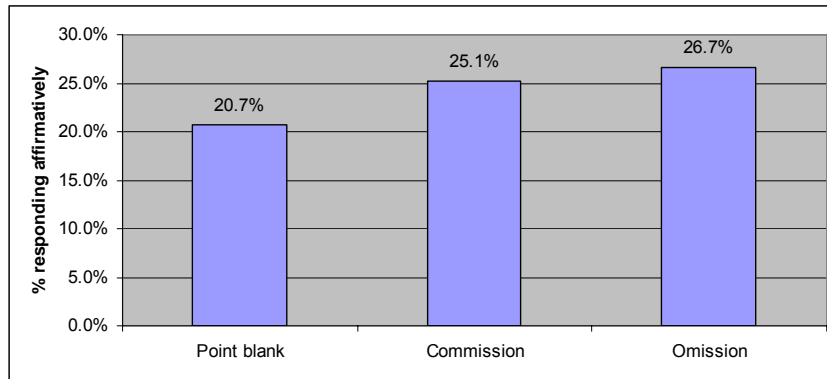
## Hypothesis

---

- Predicted disclosure rates for sensitive items:
  - Point blank < Commission < Omission



## Results: Sensitive Questions (11)



**N = 632**

**F (2, 629) = 4.68, p = 0.015**

## Sample Sensitive Questions: Percentage of Affirmative Responses

	Point blank	Commission	Omission
Having sex with the current husband, wife or partner of a friend**	8.8%	13.2%	21.7%
Having a fantasy of doing something terrible (e.g. torturing) to someone**	30.0%	48.1%	48.2%
Making a false insurance claim**	5.4%	6.8%	16.3%
Neglecting to tell a partner about a sexually transmitted disease from which one is currently suffering.*	1.7%	4.7%	8.4%
Viewing pornography when unsure whether the subjects are underage.**	21.8%	26.0%	39.2%

**X2: \*significant at p < 0.05 level; \*\*significant at p < 0.001**

## Study 3: Coherent Arbitrariness

---

- Ariely, Loewenstein, and Prelec (2003)
- Thesis: People don't have an absolute compass of the value of privacy; however, they are likely to respond sensibly to changes

## Design

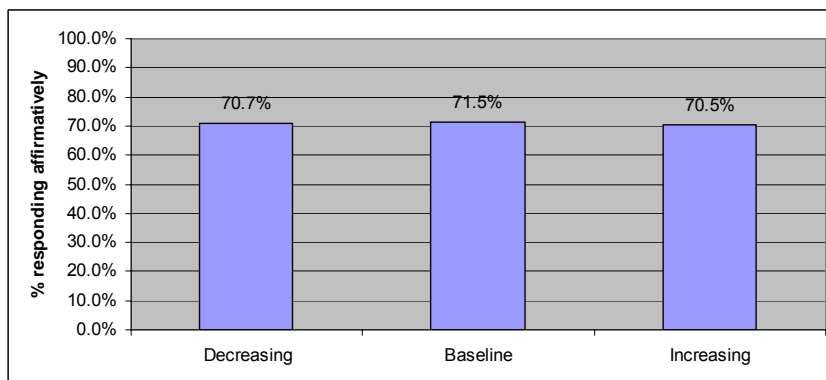
---

- Online survey posted on NY Times web site
- 30 questions ranging in intrusiveness
- 3 condition between subjects design, manipulating question order:
  - Decreasing
  - Increasing
  - Baseline (pseudorandom order of intrusiveness)

# Hypotheses

- People will anchor disclosure levels on the initial questions, but will then go on to respond coherently
- Predicted disclosure rates for intrusive items
  - Decreasing > Baseline > Increasing

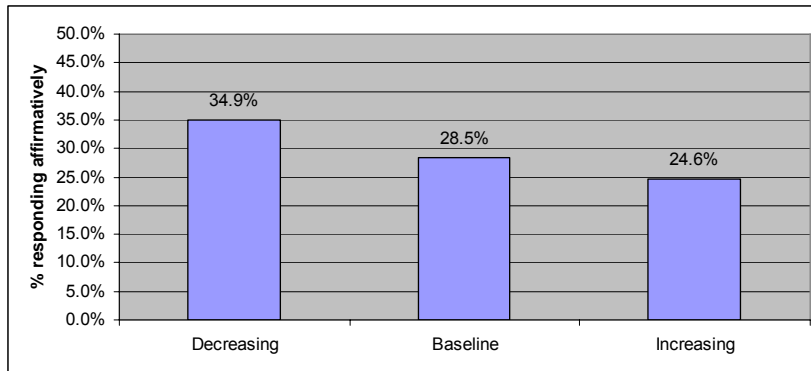
## Most Innocuous Questions (4)



**N = 1499**

**F(2,1496) = 0.32, not significant**

## Most Sensitive Questions (4)



**N = 1490**

**$F(2,1487) = 20.49, p < 0.0005$**

## Sample Sensitive Questions: Percentage of Affirmative Responses

Question	Dec.	Base	Inc.
Have you neglected to tell a partner about a sexually transmitted disease from which you were currently suffering?*	5%	4%	2%
Have you had a fantasy of doing something terrible (e.g., torturing) to someone?*	60%	41%	35%
Have you had sex with someone who was too drunk to know what they were doing?*	12%	8%	7%
Have you fantasized about having violent non consensual sex with someone?*	36%	27%	32%

**$\chi^2$ : \*significant at  $p < 0.05$  level; \*\*significant at  $p < 0.001$**

## Study 4: WTA vs. WTP

---

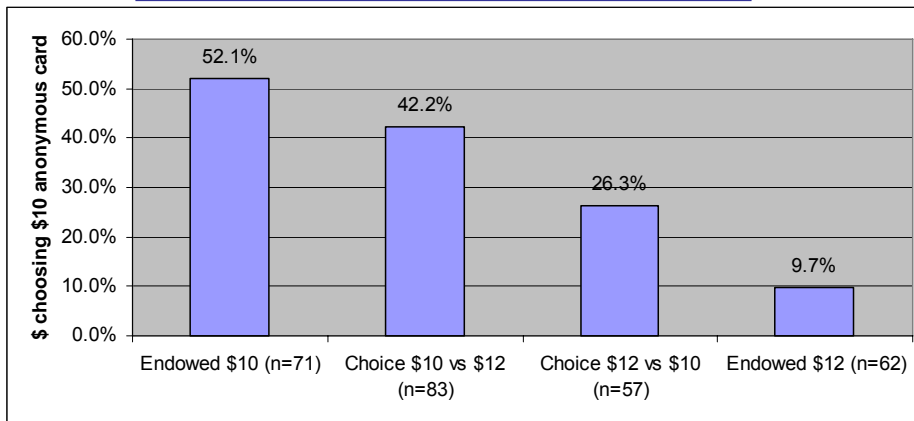
- Willingness to accept (WTP) vs. Willingness to pay (WTP)
- Gift card study: Mall patrons given choice between \$10 anonymous card and \$12 identified card
  - *Endowment*: Privacy attitudes are susceptible to endowment effect
  - *Preference uncertainty*: People's card choice will depend on subtle contextual factors, such as order of options
  - *WTA vs. WTP*: People assign different values to their personal information depending on whether they are considering **protecting it** or **revealing it**

## Design

---

- 4 condition between-subjects design
- Endowment conditions (2):
  - Endowed with \$10 anonymous card
  - Endowed with \$12 identified card
- Choice conditions (2):
  - \$10 anonymous card listed first
  - \$10 anonymous card listed second

## Results



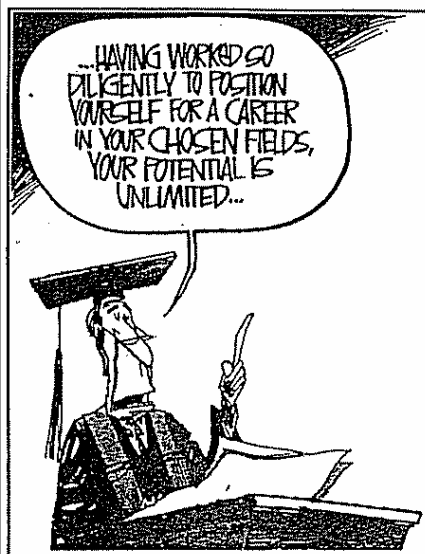
$\chi^2(3) = 30.66, p < 0.0005$

## Conclusions....

1. No consistent valuation of privacy
  - WTP/WTB study
2. Disclosure of private information is influenced by subtle contextual factors
  - Coherent arbitrariness study
3. People are not always concerned about their privacy; often their attention must be called to it
  - Assurance study
  - Overt and covert inquiries

## ... and Implications

- A behavioral perspective on concerns for privacy
  - People get more concerned about privacy when primed
  - Privacy valuations can be easily manipulated
  - Privacy behavior can be easily influenced too
  - That does **not** imply that individuals do not care about privacy
  - Behavioral economics can highlight fallacies and shortcomings in decision-making



Walt Handelsman  
Newsday  
Tribune Media Services

# References

---

- Google: [economics privacy](#)
- Visit: <http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm>
- Email: [acquisti@andrew.cmu.edu](mailto:acquisti@andrew.cmu.edu)

- 
- Backup slides



# Background

- Inconsistencies in when people reveal private information
  - Spiekermann, Grossklags, & Berendt, 2001
  - Acquisti & Grossklags
- Focus: behavioral economics applied to understanding individual concerns/behavioral responses to issues of privacy

## commission condition...

**Carnegie Mellon**

2. Pilot Survey on Ethical Standards

22%

PLEASE READ THIS NOTE! This is not the usual yada-yada!

This is a study of ethical standards.  
In the next pages, you will be presented with a series of statements describing various behaviors. We are trying to determine which types of behaviors are seen as more or less ethical. We would like you to rate the extent to which you think each behavior is unethical. (If you believe that the behavior has nothing to do with ethics, choose the "Not at all unethical" option as your answer.)

**\*\*NOTE: Because people are sometimes not objective about behaviors they have not personally engaged in, we are only interested in your ratings of behaviors in which you HAVE engaged. Therefore, ONLY IF you HAVE engaged in the given behavior (i.e. at least once), please RATE it. Otherwise, please leave all remaining items BLANK.\*\***

**Example:** Imagine that you are asked to judge how unethical it is to tell a white lie, and imagine that you have told at least one white lie in your life. You think it is only somewhat unethical. Then, in the following question, you would click on the "somewhat unethical" box.

**Telling a white lie.**

☐ Not at all unethical ☒ Somewhat unethical ☐ Quite unethical ☐ Extremely unethical

However, let's take an act that you have probably never committed: murdering someone. You believe that this is very unethical. However, in the following question, you would NOT click on the "extremely unethical" box, since you have never performed that behavior. OK?

**Murdering someone.**

☐ Not at all unethical ☐ Somewhat unethical ☐ Quite unethical ☐ Extremely unethical

\* 1. I have read and understand these instructions.  
Yes.

<< Prev Next >>

# 1. Incomplete information

---

- What information has the individual access to when she takes privacy sensitive decisions?
  - For instance, is she aware of privacy invasions and associated risks?
  - Is she aware of benefits she may miss by protecting her personal data?
  - What is her knowledge of the existence and characteristics of protective technologies?
- Privacy:
  - Asymmetric information
    - Exacerbating: e.g., RFID, GPS
  - Material and immaterial costs and benefits
  - Uncertainty vs. risk, *ex post* evaluations

# 2. Bounded rationality

---

- Is the individual able to consider all the parameters relevant to her choice?
  - Or is she limited by bounded rationality?
  - Herbert Simon's "mental models" (or shortcuts)
- Privacy:
  - Decisions must be based on several stochastic assessments and intricate "anonymity sets"
  - Inability to process all the stochastic information related to risks and probabilities of events leading to privacy costs and benefits
  - E.g., HIPAA

## Results: Demographics

- No differences between conditions in: age, education, race, likelihood of giving email
- Gender: males made more affirmative admissions than females
- Email:
  - 95% of people gave us an email address
  - 15% gave an account AND domain traceable email address

## Sensitive items: Percentage of affirmative responses

	NO assurance	WEAK assurance	STRONG assurance
Have you ever plagiarized text of any kind for an assignment?	13.8%	15.4%	3.7%
Have you ever let a classmate copy from you during an exam?	17.2%	19.2%	3.7%
Have you ever copied a classmate's homework?*	51.7%	61.5%	25.9%
Have you ever cheated on an exam?*	3.4%	26.9%	3.7%
Have you ever lied to a teacher in order to avoid taking an exam or handing in a paper on time?	10.3%	7.7%	3.7%
Have you ever lied about your grade point average?	13.8%	11.5%	3.7%

X<sup>2</sup>: \*significant at p < 0.05 level

## An alternative explanation...



## Background

- Multiple Motives Underlie Privacy
  - Similar to intertemporal choice, risk (e.g. Frederick, Loewenstein & O'Donoghue, 2002)
- Encouraging divulgence:
  - Being known
  - Intimacy
  - Group Membership
  - Self-signaling
- Discouraging divulgence:
  - Material consequences (e.g. Acquisti & Gross, 2007)
  - Qualms about revealing information

## Background

---

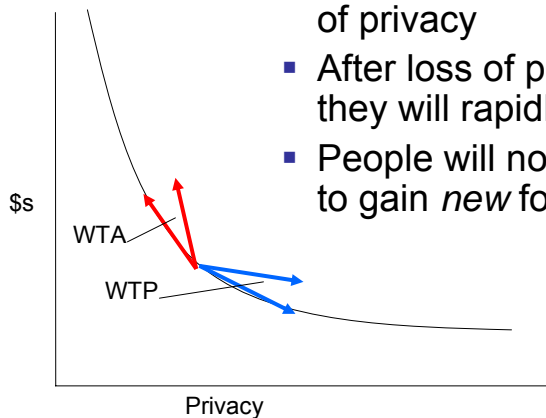
- People don't spontaneously think about privacy
  - unless you draw their attention to it
  - no consistent valuation of privacy
- What motives dominate likely to depend on subtle factors

## 1. Adaptation and loss aversion

---

- Adaptation: People become accustomed to diverse circumstances
  - Ownership
  - Wealth
  - Disabilities
- Loss aversion: People dislike losing things relative to their present circumstances, but are often relatively indifferent to gaining those same things (loss aversion)
- Also, people fail to predict these effects

## Implications for privacy



- People will initially oppose losses of privacy
- After loss of privacy, however, they will rapidly adapt
- People will not be very motivated to gain *new* forms of privacy

## 2. Time-discounting

- Ideal: people balance present and future costs & benefits in an even-handed fashion
- Reality: people place disproportionate weight on the present, relative to all future periods; 'hyperbolic time discounting'
- Especially true of
  - Young people
  - People who are in emotional states
  - People who are distracted

## Implications for privacy

---

- People won't weigh short-term benefits of divulgence against long-term consequences for privacy in even-handed fashion
  - Acquisti (2004)

## 3. Preference uncertainty & constructed preferences

---

- People don't know what they want or what they care about
  - However, people often respond sensibly to *changes* in their environment
- 'Coherent arbitrariness'

## Implications for privacy

---

- People don't have a clue about how important privacy is; however, they are likely to respond sensibly to changes



## **SSHA – A Renewal Story**

**Michael Power, Vice President, Privacy and Security, Smart Systems for Health Agency**

### **Abstract:**

Michael Power presents the recent review by the Ontario Information and Privacy Commissioner, discusses its impact and the extensive work underway to position SSHA as a leader in e-Health privacy and security.

### **Bio:**

Michael has a wealth of knowledge managing privacy and security from a legal standpoint. With over 20 years of experience, he was recently a partner at Gowling Lafleur Henderson LLP, Deputy Director of the PKI Secretariat at the Treasury Board, and various positions at the Federal Department of Justice. He has a BA, MBA and Bachelor of Laws from Dalhousie University. He was admitted to the Bar in both Nova Scotia and Ontario. In his role at SSHA, Michael leads our talented privacy and security teams and has overall responsibility for the Agency's programs in these areas.

# Privacy at SSHA

## Privacy Change Management in a Public Sector Agency



2

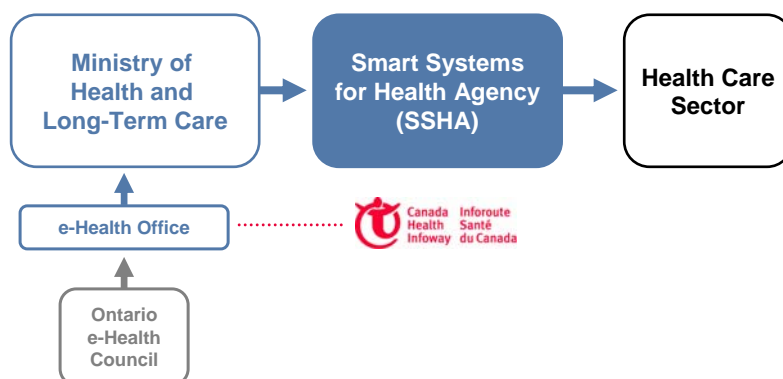
## SSHA's Unique Mandate

- Agency of the MOHLTC that operates common IT products and services for the health care system.
- SSHA helps providers share personal health information electronically between one or more health care professionals/organizations.
- Builds on existing system to expand information sharing possibilities.
- Agency plays a variety of roles:
  - HINP
  - Service provider to HINP
  - Service Provider to HIC
  - Agent of HIC
  - Institution under FIPPA

## Scope of Activities

Product	Users/User Base
ONE Network	6,600 sites
ONE ID	12,500 registered users
ONE Portal	3 portals hosted <ul style="list-style-type: none"> <li>• OntarioMD.ca</li> <li>• PublicHealthOntario.ca</li> <li>• eHealthOntario.ca</li> </ul>
ONE Hosting	15 applications hosted
ONE Mail	65,000 users

## e-Health in Ontario



## SSHA: Change within Change

- Reorganization objectives:
  - Build on existing strengths.
  - Add corporate capability eg Enterprise Architecture.
  - Strengthen core functions eg Project Management, Client Management.
  - Clarify roles, functions, and accountabilities.
  - Become more customer focused.
  - Become scalable (to accommodate growth in scale and complexity).



## IPC Review – released March 2007

- First organization to be reviewed by IPC under PHIPA legislation.
- No other agency in Canada has gone through such an extensive review.
- 82 Recommendations.
- Findings:
  - No breaches
  - Need for detailed plan to improve and update SSHA's program.

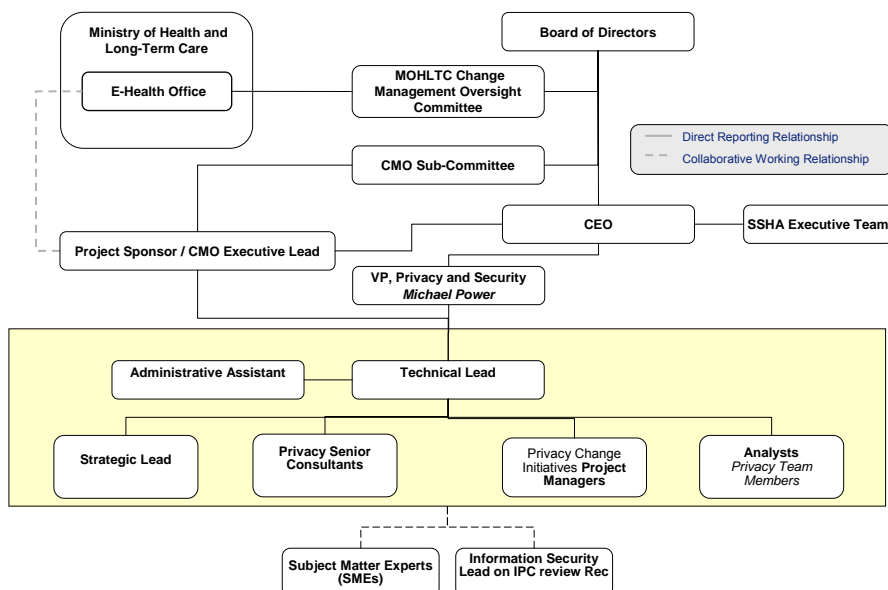
## Response goals

- Update relevant policies and procedures.
- Embed privacy and security deeper into our organizational culture.
- Improve transparency by making privacy and security solutions available to clients.

## SSHA Approach to IPC Report

- Conducted analysis of recommendations.
- Identified owners and high level approach.
- Established Privacy Change Initiative Project Management Office (PCIPMO).
- Completed detailed planning and resourcing exercise.
- Began implementation phase.
- Emphasized continuous improvement.

## PCIPMO Governance and Reporting Structure



## IPC Review Recommendations to Sub-Stream Mapping

	Sub-Stream	Recommendations
1. Privacy	1.1. Policy and Procedures	R1,R5,R6,R7,R8,R10,R34,R36,R37,R38,R43,R52,R67,R68
	1.2. Training Content	R4,R45,R52
2. Security	2.1. Policy and Procedures	R1,R3,R5,R6,R7,R9,R10,R11,R12,R13,R14,R15,R46,R48
	2.2. Incident Management	R66
	2.3. Training Content	R52
3. Risk Management	3.1. Risk Management Program	R20,R21,R22,R73,R74,R75,R77,R78,R79
	3.2. BCP and DRP	R65
4. Asset Management	4.1. Policy and Procedures	R15,R16,R17,R70
5. Products & Services	5.1. PIA Updates	R35,R39,R40,R41,R42,R45
	5.2. TRA Updates	R47,R49
	5.3. Supporting Controls	R11,R12,R44,R51,R56,R63,R64,R69
	5.4. Documentation and Communication	R11,R54,R59,R61,R62
6. Framework	6.1. Policy	R1,R18,R23
	6.2. Method	R10,R12,R36,R37,R38,R39,R40,R41,R42,R43,R45,R48,R49,R50,R71,R76
	6.3. Supporting Controls	R2,R19,R20,R21,R22
	6.4. Training Solution	R4,R52,R53
7. Governance	7.1. Culture	R80
	7.2. Roles and Responsibilities	R3,R4,R7
	7.3. Reporting, Monitoring and Compl.	R72,R81,R82
8. Client Management	8.1. Agreements	R30,R32
	8.2. Client Communications	R35,R36,R37,R47,R48,R55,R57,R58,R60,R62,R69
	8.3. Supporting Controls	R31,R33
9. Vendor Management	9.1. Agreements	R24,R25,R26,R27,R28
	9.2. Vendor Privacy Program	R8,R10,R25,R26,R27,R29

## How we responded – summary

- 70% of recommendations completed by 30 September 2007.
- 84% to be completed by 31 March 2008.
- Balance requires consultation with external partners.
- October 2007: Independent review by IPC.
  - David Flaherty Report.

## IPC response – other progress

- Consultations with:
  - Chief Information and Privacy Officer of the Ministry of Government Services
  - e-Health Program
- CEO-initiated consultation with clients, included consultation on privacy issues.

## Continuous Improvement

- Privacy culture strategy finalized.
- Privacy procedures finalized.
- Policy for PIAs and reviews refreshed and finalized.
- Data removal and media disposal process and procedures finalized.
- Privacy Impact Assessments updated for generally available products and services, including Network Refresh and ONE OfficeNET.
- Launch of online Learning Management System (LMS) covering Privacy and Information Security.
- Launch of Enterprise Security and Privacy Incident Management Program.
- Revision of Information Classification and Handling policy as an Agency standard.
- Implementation of Information Classification Guidelines.
- Finalization of privacy and security aspects of procurement documentation.



## Next Steps

- Continue implementing as planned.
- Continue to work with IPC.
- Continue to consult with client stakeholders.
- Expand on the implementation work and build a best practice program.
- Deepen our privacy culture.

## Staff awareness campaign

- September 2007 launch
- Tied to:
  - Updated Privacy and Security Standard of Conduct.
  - Updated Information Security Policy.
  - Strengthened document management practices
  - Mandatory staff training.
  - Enterprise Security and Privacy Incident Management Planning.

## Staff awareness campaign – goals

- Raise profile of Privacy and Security staff and function:
  - “Desk tour”
  - Poster campaign
  - Telephone hotline and central e-mail
- Reward positive actions defined in Standard of Conduct.



# Privacy Training

## Privacy Legislation and Incident Handling

**Module:** Introduction

**Module Overview:**

**Module Objectives:**

**Legal Requirements:**

**Privacy and Security Standard of Conduct:**

**CSA Model Code:**

**SSHA's Roles & Responsibilities:**

**Privacy Incidents:**

**Privacy and Security Incident Response Process:**

**Outcomes of a Privacy Investigation:**

**Oversight, Penalties and Offences:**

**Reference Materials:**

**Module Summary:**

### Before We Begin...

Before we begin this module, let's take a moment to discuss the navigation controls and interactive elements.

This module has been designed so that you may complete the content at your own pace. The navigation bar at the bottom of the page (shown here) lets you move forward and backward within the module.

A number of image buttons can be found throughout the lesson. These buttons activate additional content. To see an example, please click the buttons to the right.

Your lesson progress will be shown at the bottom left of the screen, and the index at the left side shows you the topics covered in this module. The current topic will be shown in black.

When you are ready to move forward in the module, click the "Go To Next Step" button on the navigation bar below.

You are currently on Step 0 of 13

Page 1 of 41

# Privacy Training

## Privacy Legislation and Incident Handling

**Module:** Introduction

**Module Overview:**

**Module Objectives:**

**Legal Requirements:**

**Privacy and Security Standard of Conduct:**

**CSA Model Code:**

**SSHA's Roles & Responsibilities:**

**Privacy Incidents:**

**Privacy and Security Incident Response Process:**

**Outcomes of a Privacy Investigation:**

**Oversight, Penalties and Offences:**

**Reference Materials:**

**Module Summary:**

### Oversight, Penalties and Offences

The Commissioner's mandate is to provide an independent review of the decisions and information practices of government organizations, including SSHA, as an agency of the Ministry of Health and Long Term Care (MOHLTC).

**The Information and Privacy Commissioner/Ontario is an oversight body that:**

- Adjudicates access appeals and investigates privacy complaints
- Monitors compliance with privacy requirements of FIPPA and PHIPA
- Makes comments and recommendations on privacy implications of any matter under review

**FIPPA and PHIPA offences for certain willful contraventions:**

- FIPPA: If found guilty of an offence, fines of up to \$5,000 are imposed
- PHIPA: Maximum penalty of \$50,000 for individuals and \$250,000 for the Agency

**IPC Links:**

- For the IPC website, visit <http://www.ipc.on.ca>
- For questions or comments to the IPC, contact [info@ipc.on.ca](mailto:info@ipc.on.ca)

Dr. Ann Cavoukian

You are currently on Step 13 of 13

Page 35 of 41

# Privacy Training

The screenshot shows a web-based training module interface. On the left is a vertical navigation menu with the following items: Module Introduction, Module Overview, Module Objectives, Legal Requirements, Privacy and Security Standard of Conduct, CSA Model Code, SSHA's Roles & Responsibilities, Privacy Incidents, Privacy and Security Incident Response Process, Outcomes of a Privacy Investigation, Oversight, Penalties and Offences, Reference Materials, and Module Summary (which is highlighted). The main content area is titled 'Privacy Legislation and Incident Handling' and 'Module Summary'. It includes a 'Congratulations!' message stating that the user has successfully completed the self-paced online module. Below this, it lists five key responsibilities for SSHA staff: Describe SSHA's privacy roles and responsibilities, Understand key SSHA terms and definitions, Identify a privacy incident and act accordingly, Continue to protect privacy, and Contribute to building a privacy culture at SSHA. A note mentions that to certify completion of the annual Privacy Fundamentals program, a 90% pass score on the quiz is required. At the bottom, it says 'You may now exit the lesson using the "Exit Module" button at the bottom of the page.' A large, semi-transparent 'SUMMARY' watermark is visible in the background. At the very bottom, a status bar indicates 'You are currently on Step 13 of 13' and 'Page 41 of 41'.

## Role of Privacy and Security Team

- Core mandate: Protect sensitive information from unauthorized or accidental access, use or disclosure.
- How? By ensuring SSHA products, services and processes:
  - Are well designed.
  - Meet obligations under government legislation.
  - Properly protect rights of patients and health care providers.
- Work with Information Privacy Commissioner (IPC) of Ontario to continuing improve privacy activities.
- Role within SSHA evolving.

## What all this means

- SSHA's objective is to become health care sector's IT provider of choice
  - Gaining, keeping and building trust
- We will continue evolving and innovating to protect information entrusted to Agency.
- We will be transparent so you can learn from and leverage our experiences.

## Questions?

Michael Power  
Vice President, Privacy and Security  
Smart Systems for Health Agency  
[michael.power@ssha.on.ca](mailto:michael.power@ssha.on.ca)

## **Session 1A: De-identification Techniques**

**Chair: Khaled El Emam, CHEO RI and University of Ottawa**

### **Session Overview:**

There is growing demand for health data sets for research, quality improvement, and surveillance. The privacy concerns around the sharing of this data are complex, and often result in the most cautious approach being followed (i.e., no disclosure allowed). In this session, we will present the latest developments in the de-identification of clinical and DNA data, and examples of the application of de-identification techniques in practice.

### **Biography of Chair:**

Dr. Khaled El Emam is an Associate Professor at the University of Ottawa, Faculty of Medicine and the School of Information Technology and Engineering. He is a Canada Research Chair in Electronic Health Information at the University of Ottawa. Previously Khaled was a Senior Research Officer at the National Research Council of Canada, and prior to that he was head of the Quantitative Methods Group at the Fraunhofer Institute in Kaiserslautern, Germany. In 2003 and 2004, he 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. He holds a Ph.D. from the Department of Electrical and Electronics, King's College, at the University of London (UK). His lab's web site is: <http://www.ehealthinformation.ca/>.

# **Patient Re-identification and Anonymity Protection in Clinical Genomics Research**

**Brad Malin, Vanderbilt University, USA**

## **Abstract:**

Decreasing costs in information and high-throughput technologies have facilitated an explosion in the collection and analysis of person-specific clinical and genomic data. To capitalize on the opportunity, many organizations around the world are building databanks that integrate, store, and enable access to massive quantities of biomedical records for research purposes. At the same time, the dissemination of such records must protect a subjects' anonymity, so various technologies have been proposed to "de-identify", or remove, personal identifiers such as names and residential addresses that are initially associated with the data. However, in this talk I will illustrate that many seemingly anonymous DNA records can be "re-identified" to named individuals in public resources with relatively little effort through simple automated strategies. In fact, I will show that anonymity is compromised through a number of mechanisms that take advantage of residual inferences in de-identified DNA and clinical records, as well as various public data collections. Despite the susceptibility of many data protection technologies, I will then present how we can design and implement formal anonymity protection without preventing the scientific uses of databases. This talk will investigate the interplay between technology and policy issues at play in the protection of person-specific genomics data.

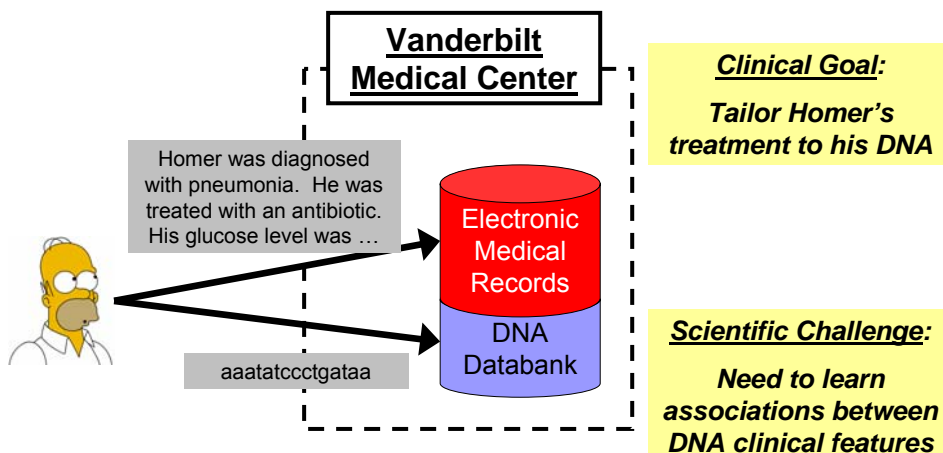
## **Bio:**

Bradley Malin is an Assistant Professor of Biomedical Informatics in the School of Medicine at Vanderbilt University and holds a secondary appointment in the School of Engineering. He received a bachelor's degree in molecular biology, a master's degree in knowledge discovery and data mining, a master's in public policy and management, and a doctorate in computer science, all from Carnegie Mellon University. He is the author of numerous scientific articles on biomedical informatics, data mining, and data privacy. His research in genetic databases and privacy has received several awards from the American and International Medical Informatics Associations. He has chaired and served as program committee member for various workshops and conferences on healthcare, privacy, and data mining. From 2004 through 2006 he was the managing editor of the Journal of Privacy Technology (JOPT) and he is the guest editor for an upcoming special issue on privacy and data mining for the journal Data and Knowledge Engineering.

# Patient Re-identification and Anonymity Protection in Clinical Genomics Research

Bradley Malin, PhD  
Assistant Professor of Biomedical Informatics  
Vanderbilt University  
December 3, 2007  
b.malin@vanderbilt.edu

## Your Data is Collected





# Genetic Association Approaches

## Traditional Model

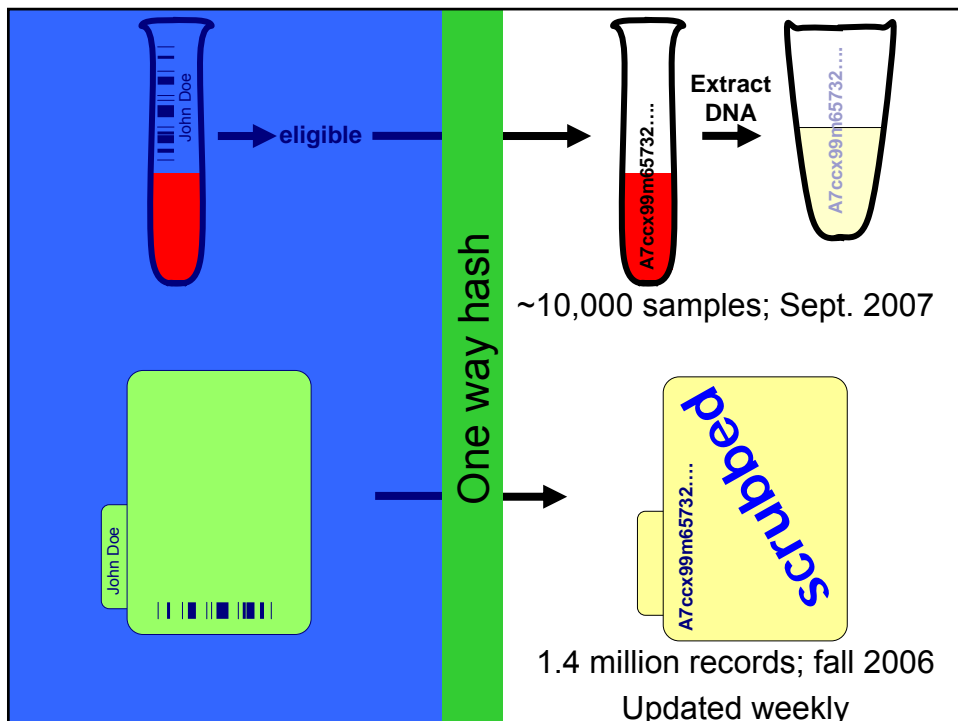
- Disease specific
- Defined population
- Investigator driven
- Specific hypothesis
- Smaller populations
- Research derived samples and information
- Candidate genes specific to disease
- Subjects can be recontacted
- **Hypothesis testing**

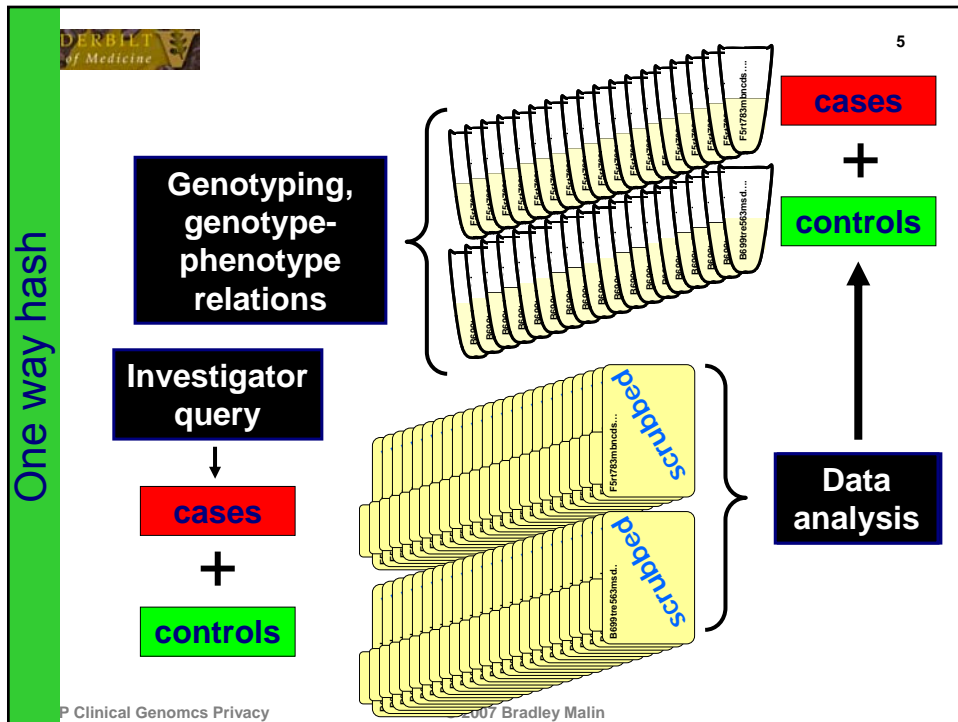
## Vanderbilt DNA Databank Model

- Any disease
- All comers
- Institutionally managed
- Multiple/dynamic hypotheses
- Large scale
- Clinically derived samples and information
- Genome scan, shared genotyping database
- De-identified
- **Hypothesis generation**

EHIP Clinical Genomics Privacy

© 2007 Bradley Malin





**VANDERBILT School of Medicine**

6

## The Vanderbilt DNA Databank

- Institutionally funded project
- DNA extraction from leftover blood
  - 25K-75K per year, 250K within 5 years
- Non-human subjects research
  - Samples & data not linked to identity
  - Conducted with IRB & ethics oversight

EHIP Clinical Genomics Privacy

© 2007 Bradley Malin

VANDERBILT School of Medicine 7

## Example De-identified Medical Record

The screenshot shows a medical record interface with several red callout boxes and arrows pointing to specific areas:

- MR# is removed:** Points to the patient ID field.
- Substituted names:** Points to the patient name field.
- Replaced SSN and phone #:** Points to the social security number and phone number fields.
- Unknown residual re-identification potential (e.g. "the mayor's wife"):** A large black box with white text covering the patient's name and other identifying information.
- Shifted Dates:** Points to the date of birth field.

The medical record text includes:

ONCOLOGY CLINIC NOTE 2004/09/28  
 Signed by: \*\*\*\*\*  
 SMITH, JILLIAN (02/01/1949)  
 DIAGNOSIS: Stage II invasive mammary breast cancer "T2 N0 M0"  
 ONCOLOGIC HISTORY: Dr. Smith is a 55-year-old female who is post-menopausal who was found to have an abnormality on her mammogram. She subsequently had an ultrasound-guided FNA which showed malignant cells. She was referred to the breast Center where she underwent a core biopsy on August 30, 2004, which showed infiltrating mammary carcinoma. She subsequently was seen by Dr. Owens who, on August 30, 2004, did a left modified radical mastectomy. Pathology from this revealed an invasive mammary carcinoma, no special type, with lobular features, 2.2 cm in greatest dimension, which was intermediate combined histologic grade with low proliferative rate. Tumor extending to 2 mm in the lower, lateral, deep margin. There was no evidence of lymphovascular invasion present. Thirteen lymph nodes were negative for malignancy. Her tumor was ER positive, PR positive and/or negative. She, at the time of surgery, had placement of a tissue expander. For immediate first operation reconstruction of her left breast, by Dr. McDonald. It was decided since her final pathology showed tumor extending to 2 mm from the lower, lateral deep margin, that she be referred to Willburn Clouse who was planning on doing radiation therapy after she received chemotherapy. She had a BSA test done on September 28, 2004, which showed a normal ejection fraction with a left ventricular ejection fraction of 50%. She is here to receive her first cycle of Adriamycin and Cyclophosphamide. We discussed the risks and benefits of chemotherapy and she has decided to proceed with chemotherapy.

REVIEW OF SYSTEMS:  
 General: Denies weakness, fatigue, fever, anorexia, or itching.

EHIP Clinical Genomics Privacy © 2007 Bradley Malin

VANDERBILT School of Medicine 8

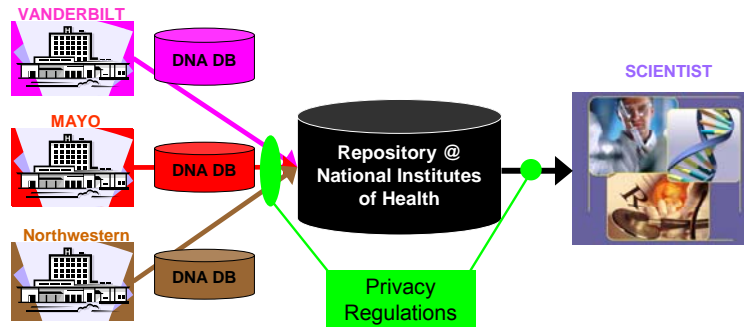
## Technology + Policy

- Databank access restricted to Vanderbilt employees
  - it is NOT a public resource
- Databank users sign Data Use Agreement that prohibits use of data for re-identification
- Access approved on project-specific basis by Operations Advisory Board (OAB) and Institutional Review Board
- Project-specific user ID and password; all data access logged and audited by OAB

EHIP Clinical Genomics Privacy © 2007 Bradley Malin

## Beyond the Institution

- **Goal:** Construct repositories of person-specific genetic data for biomedical, epidemiology, pharmacogenetic research



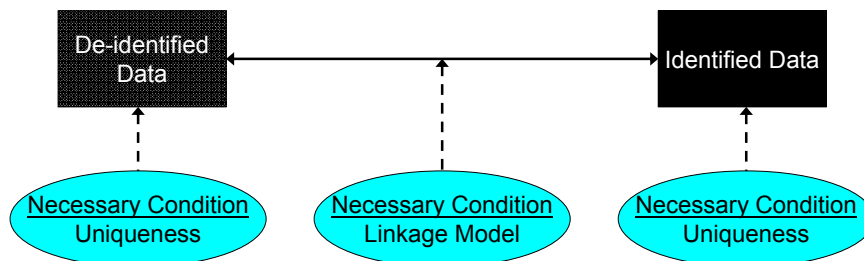
- **Challenge:** Data collectors need to contribute, but worry data will be re-identified to named individuals

## Competing Policies

- Feb '03: National Institutes of Health Data Sharing Policy
  - *“data should be made as widely & freely available as possible”*
  - *researchers who receive  $\geq \$500,000$  must develop a data sharing plan or describe why data sharing is not possible*
- Aug '06: NIH Supported Genome-Wide Association Studies Policy
  - *Derived data must be shared in a manner that is devoid of “identifiable information”*

# Re-identification?

## Central Dogma of Re-identification



## HIPAA - Secondary Data Sharing

- Safe Harbor
- Limited Release
- Statistical or Scientific Standard

## HIPAA Safe Harbor

- Data that can be given away by a covered entity
- Requires removal of eighteen direct and other “quasi-”identifiers
  - 1) Name / Initials
  - 2) Street address, city, county, precinct code and equivalent geocodes
  - 3) All ages over 89
  - 4) Telephone Numbers
  - 5) Fax Numbers
  - 6) Electronic Mail Address
  - 7) Social Security Number
  - 8) Medical Record Number
  - 9) Health Plan ID Number

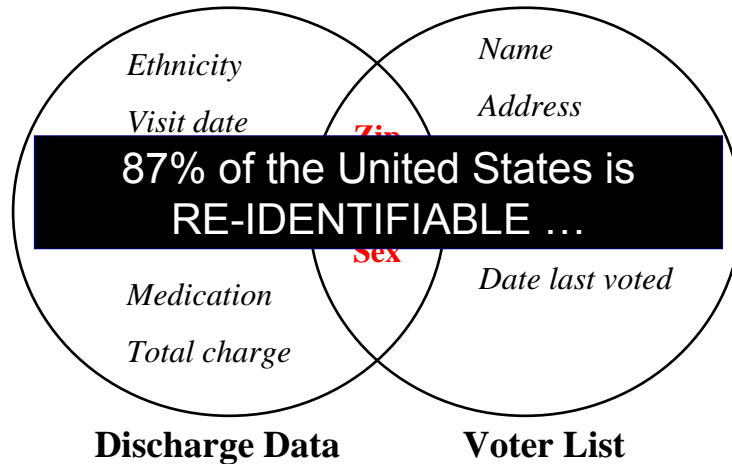
## HIPAA Safe Harbor

- Safe Harbor (cont'd)
  - 9) Account Number
  - 10) Certificate / License Number
  - 11) Vehicle identifiers and serial numbers, including license plate numbers
  - 12) Device Identifiers and serial numbers
  - 13) Web addresses (URLs)
  - 14) Internet IP Addresses
  - 15) Biometric identifiers, including finger and voice prints
  - 16) Full face photographic images and any comparable images
  - 17) Any other unique identifying number, characteristic, or code
    - A code is an identifier if the person holding the coded data can re-identify the individual

## HIPAA Limited Data Set

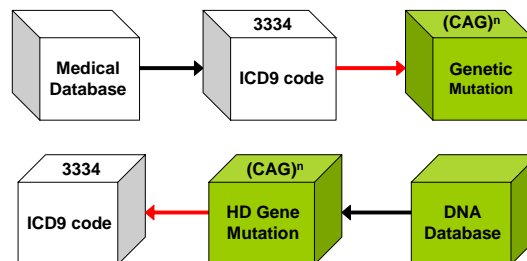
- Includes more specific information than Safe Harbor Dataset
- Can include
  - ☐ Dates of birth
  - ☐ Dates of death
  - ☐ Dates of service
  - ☐ Town or city
  - ☐ State
  - ☐ Zip code
- **Requires Contract:** Research entity provides assurances that it will not use or disclose the information for purposes other than research and will not identify or contact the individuals who are the subjects

# Linking to Re-identify Data (Sweeney 1997, 1998)



# DNA Re-identification

- Many deployed genomic privacy technologies leave DNA susceptible to re-identification (Malin, JAMIA 2005)
- DNA is re-identified by automated methods, such as:
  - Genotype – Phenotype Inference (Malin & Sweeney, 2000, 2002)



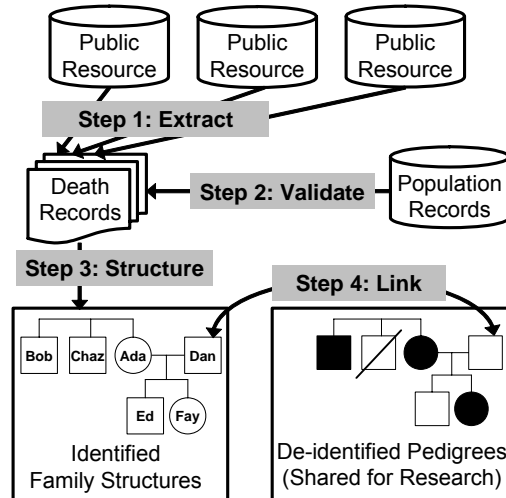


# Genealogy Re-identification

(Malin 2006)

## ■ *IdentiFamily*:

- software program that links de-identified pedigrees to named individuals
- Uses publicly available information, such as death records, to build genealogies



# Genealogy Re-identification

(Malin 2006)

The screenshot shows a news article from WyomingNews.com, specifically the obituary for Richard R. Mann. The article is titled "OBITUARIES" and "Richard R. Mann". It includes the following text:

1924-2007

Richard R. Mann, 82, of Cheyenne died Jan. 12 at Cheyenne Regional Medical Center. He was born June 29, 1924, in Allentown, Pa., and had lived here since 1956.

Mr. Mann served in the Army Air Corp during World War II in South Africa and Italy. He retired as a flight engineer for the Wyoming Air National Guard.

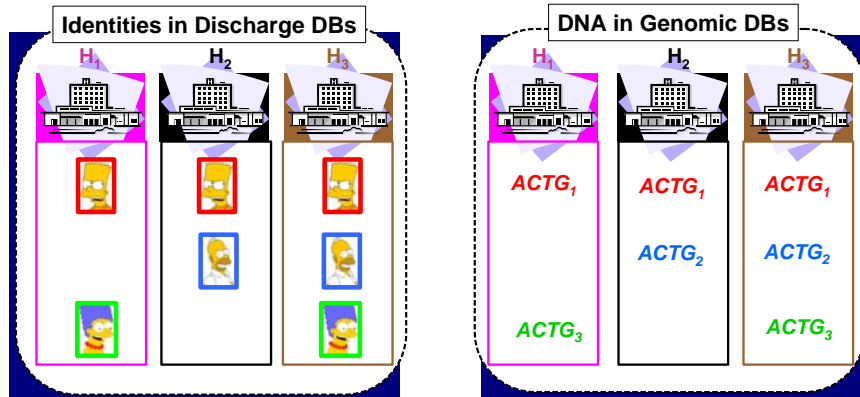
Mr. Mann was a member of St. Mary's Catholic Church, Elks, Moose and the Knights of Columbus, where he had been a past grand knight and state deputy.

He is survived by two sons, Gerald Mann and Thomas Mann, both of Cheyenne; seven daughters, Teresa Johnson, Kathryn Schroll, Judith Oldenburg, Cheryl Thibault, and Jon Cameron, all of Cheyenne; Lou Ann Golden of Sidney, Neb., and Kimberly Byron of Littleton, Colo.; his companion, Katie Heaton of Cheyenne; 25 grandchildren and two great-grandchildren.

He was preceded in death by his wife of more than 50 years, Patricia A. Mann; two daughters, Mary Constance Grant and Jeanane Rhodes; his parents, Russell and Viola Mann; two brothers, Roland Mann and Robert Mann; and a sister, Rochelle Behrandt.

## Trails!

(Malin & Sweeney, 2001; 2004, 2005, Malin & Airolidi 2006, Malin 2007)



## Privacy Fears Cause Adverse Effects

- Investigators surveyed about pedigrees published in journals (Botkin et al 1998)
- 177 investigators:
  - ☐ 78% did not obtain informed consent
  - ☐ 7% obtained consent from all family members
  - ☐ 36% did not inform family members of publication
  - ☐ **20% altered pedigrees before submission**
    - **50% did not tell editors**

# Protection?

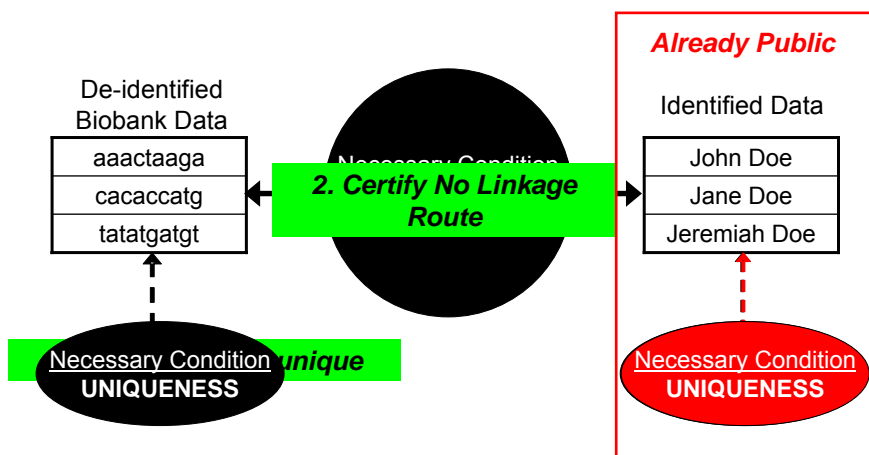
## HIPAA - Secondary Data Sharing

- Safe Harbor
- Limited Release
- Statistical or Scientific Standard

## HIPAA Statistical / Scientific Standard

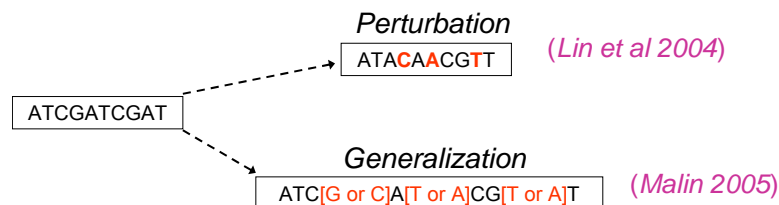
- Certify via “*generally accepted statistical and scientific principles and methods, that the **risk is very small** that the information could be used, alone or in combination with other reasonably available information, by the anticipated recipient to identify the subject of the information*”
- “**Must document the methods** and results of the analysis that justify such a determination”
- “**Must not disclose the key** or other mechanism that would have enabled the information to be re-identified”
  - includes pseudo-random number algorithms and seed values

## Understanding Re-identification

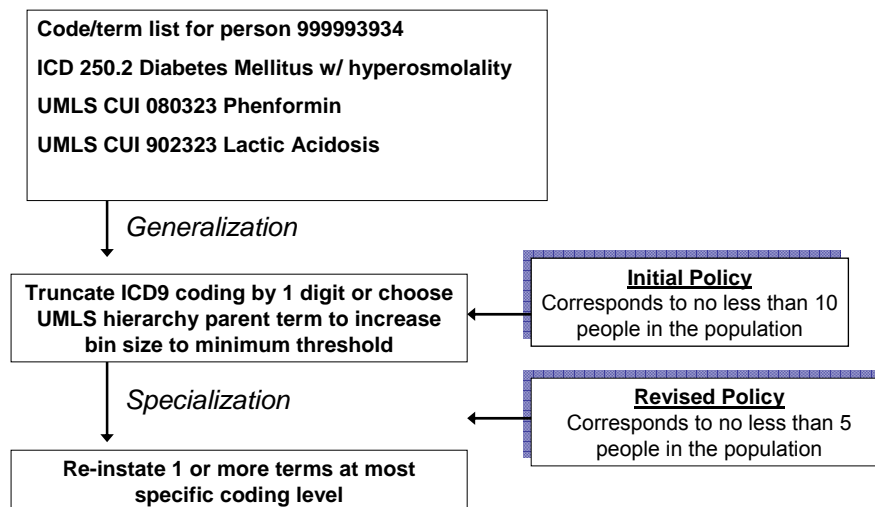


# Uniqueness: Beyond Ad hoc Protections

- Perturbation does not guarantee privacy
- Alternative: Generalization of data
  - Retains semantics
  - Given enough data – can reconstruct aggregate distributions and associations



## Generalization / Specialization of EMR coded data



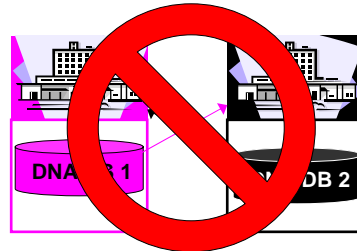
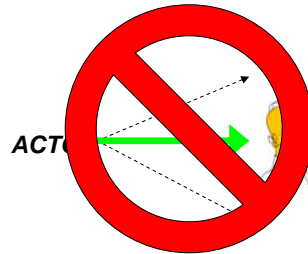
# Formal Protection Models

- **$k$ -Map** (Sweeney, 2002)
  - Each shared record refers to at least  $k$  entities in the population
- **$k$ -Anonymity** (Sweeney, 2002)
  - Each shared record is equivalent to at least  $k-1$  other records
- **$k$ -Unlinkability** (Malin 2006)
  - Each shared record links to at least  $k$  identities via its trail
  - Satisfies  $k$ -Map protection model

## From Re-identification to Protection A Trails Example

## Detection → Protection

- We now know what constitutes a trail re-identification, but how can we prevent it?
- Challenges to Overcome:
  - **Challenge #1:** Must prove DNA trail can not be re-identified to named person
    - Satisfy HIPAA requirement
  - **Challenge #2:** Can not force sharing of data
    - Confidentiality issues

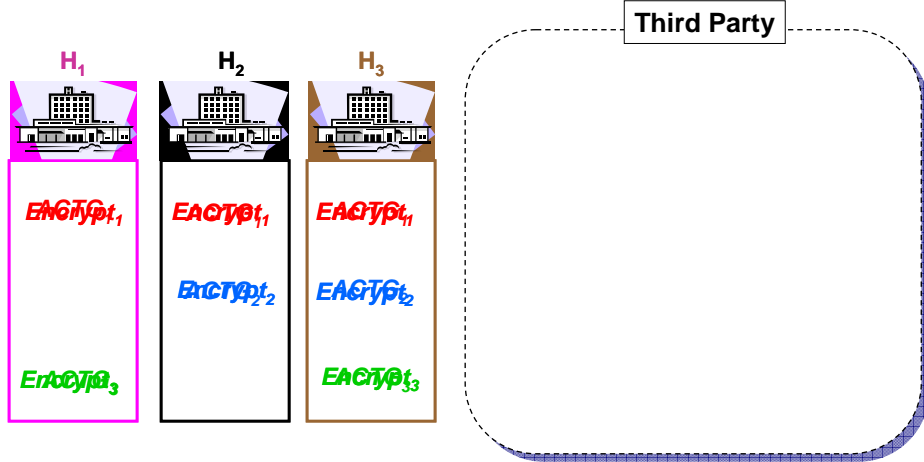


## A Solution: STRANON

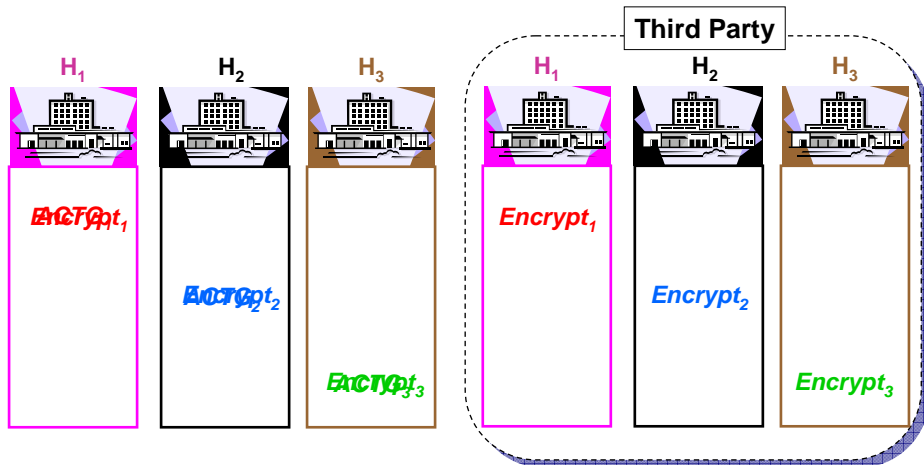
*(Malin & Sweeney, AMIA 2005, ICDE 2006)*

- Secure Trail Anonymization
  - Prevent trail re-identification by guaranteeing data satisfies  $k$ -unlinkability
    - Guarantees every DNA trail is linkable to  $\geq k$  identity trails
  - Enable communication using a novel secure multiparty computation protocol via a third party *(Malin et al, ICDE 2005)*
    - DNA is encrypted until it is  $k$ -unlinkable

# Simple Walkthrough

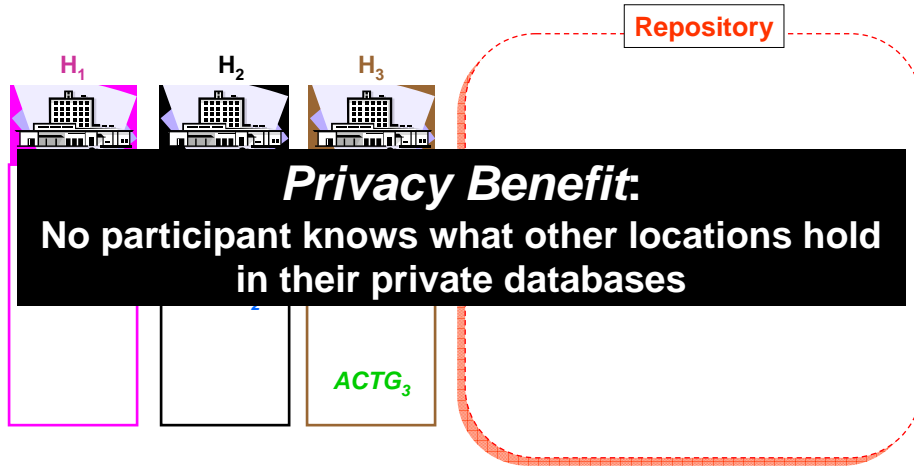


# Simple Walkthrough





## Simple Walkthrough



## Experimental Validation

(Malin & Sweeney JBI 2004, AMIA 2006, Malin AIIM 2007)

- Illinois hospital discharge databases (1990-1997)
- Approx. 1.3 million hospital discharges per year
- Compliance with  $\geq 99\%$  of discharges in IL hospitals
- Extracted datasets for seven Mendelian disorders
  - ☐ Cystic fibrosis (CF)
  - ☐ Phenylketonuria (PK)
  - ☐ Friedrich's Ataxia (FA)
  - ☐ Sickle Cell Anemia (SC)
  - ☐ Huntington's Disease (HD)
  - ☐ Tuberos Sclerosis (TS)
  - ☐ Hereditary Hemorrhagic Teleangiectasia (HHT)

## Before STRANON, $k = 5$

**Re-identified:** DNA trail maps to  $< k$  identities

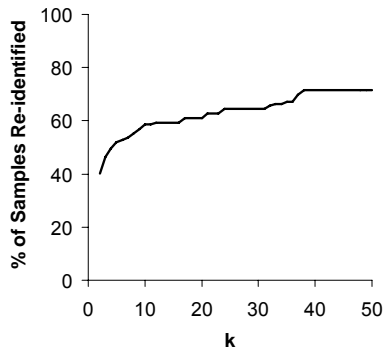
Dataset	Samples	Hospitals	% $k$ -Re-identified	% in Repository
TS	220	119	93%	100%
FA	129	105	92%	100%
PK	77	57	91%	100%
HD	419	172	90%	100%
HT	429	159	84%	100%
CF	1149	174	52%	100%
SC	7730	207	38%	100%

## After STRANON, $k = 5$

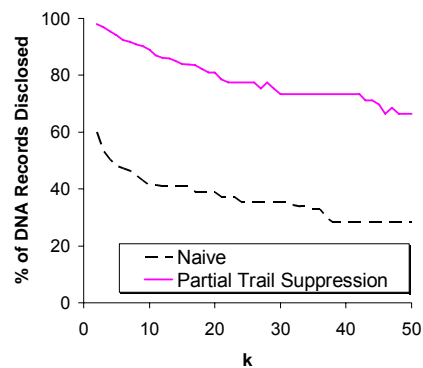
**Re-identified:** DNA trail maps to  $< k$  identities

Dataset	Samples	Hospitals	% $k$ -Re-identified	% in Repository
TS	220	119	0%	78%
FA	129	105	0%	76%
PK	77	57	0%	60%
HD	419	172	0%	93%
HT	429	159	0%	88%
CF	1149	174	0%	98%
SC	7730	207	0%	99%

## A Closer Look: Cystic Fibrosis (1149 samples)

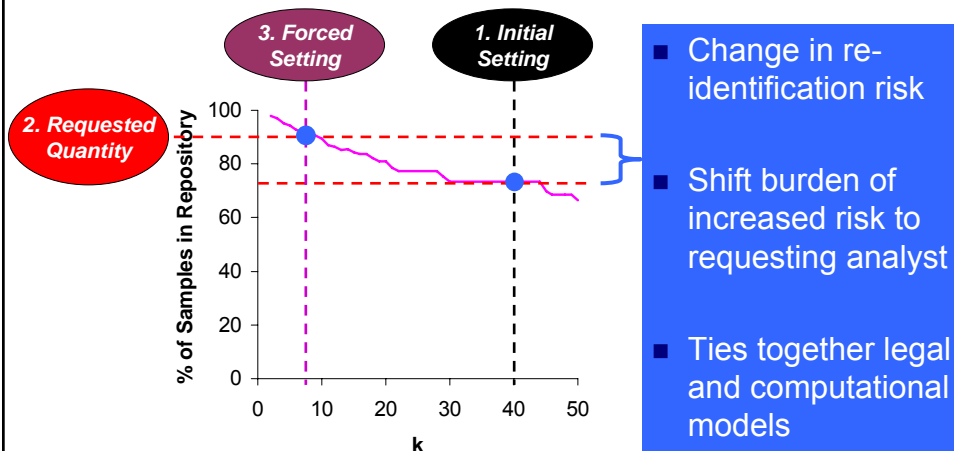


**BEFORE STRANON**  
100% Samples In Repository



**AFTER STRANON**  
0% Samples k-Re-identified

## Benefit: Quantified Risk



# Conclusions

- Looks are only skin deep
  - Databases that say they protect data privacy must have proof
- Re-identification threats exist
  - Attacks, such as trails, are automated, systematic, and non-trivial
- Don't Be Naïve
  - Formal protection systems can and should be built
  - Need a new paradigm: solutions that merge biomedical knowledge, computational methods, and public policy
- More To Do
  - Problems left to solve (e.g., formal anonymity protection for text), but the potential and opportunity is there

# De-identifying Data for Health Research and Surveillance

**Khaled El Emam, University of Ottawa**

## **Abstract:**

The use of electronic medical records is increasing. EMR data is also a valuable source of information for health research and disease surveillance. A typical pre-condition for disclosing clinical and identifying data is for it to be de-identified. When does information cease to identify an individual? Conversely, what is the minimum amount of information needed to identify an individual? Through a series of studies we evaluated the risk of re-identification using public sources. This talk presents an overview of our findings and illustrates how these can be used to perform risk assessment in various situations. Based on the results, we can also make some recommendations on safe de-identification practices. This presentation would be of interest to policy makers, statisticians, clinical researchers, and computer sciences working in the security and privacy area.



# De-identification Methods

**Khaled El Emam**  
*University of Ottawa*



## Issues in de-identification

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- This is risk based – we need to have an ability to assess re-identification risks properly
- De-identification always entails the loss of information – we cannot ignore that
- The answer will be different each time – optimal de-identification will depend on the specific case under consideration
- Current practices are quite simple – we may be tricking ourselves into believing that the risks are being managed

v1.3 - 2  
Khaled El Emam –De-identification Methods

## Do We Need to De-identify ? - I

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Good security and good contracts are a good start – necessary but insufficient conditions:
  - Insider attacks (disgruntled employees, blackmail, fraud)
  - It is not possible to control carelessness and staff who do not follow procedures (this will happen)
  - There will be a negative business reaction to the usability problems introduced from too much security, esp. in private enterprises

v1.3 - 3

Khaled El Emam –De-identification Methods

## Do We Need to De-identify ? - II

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Even reputable and highly respected people make mistakes

“There are few Canadian examples of harms associated with the use of personal health data for administrative and research purposes by publicly funded institutions. In general, health data are well protected by the health care system and provide an admirable example of public trust. [...] Thus far, researchers, administrators and health care providers in Canada have an excellent record of protecting the confidentiality of health data.”

Upshur et al., CMAJ, 165(3):307-309, 2001

v1.3 - 4

Khaled El Emam –De-identification Methods

## Do We Need to De-identify ? - III

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- On 4<sup>th</sup> January 2007, 2900 records lost in a laptop from Sick Kids (HO-004)
- Data leaks through second hand computers
- Researchers do not have perfect record management practices
- Poor passwords to protect PHI in clinical research

v1.3 - 5  
Khaled El Emam –De-identification Methods

## De-identification steps

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Remove identifying information
- Define the risk threshold
- Define the quasi-identifiers
- What is the risk of uniqueness ?
- What is the risk from matching ?
- De-identify the quasi-identifiers

v1.3 - 6  
Khaled El Emam –De-identification Methods



## Identifying information

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- These are obvious variables, like name, address, telephone number, SIN
- These should be removed completely if not needed
- Randomization can be used where the field needs to have some values, but not necessarily real ones
- Coding can be used where removal may need to be reversed (eg, clinical trials: adverse events and notification of +ve results)

v1.3 - 7

Khaled El Emam –De-identification Methods

## Risk Threshold

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- This is the maximum risk of re-identification that the custodian is willing to tolerate:
  - Type of risk you are worried about:
    - How many individuals in your data set can be re-identified ?
    - What is the acceptable probability of that actually happening ?
  - Would the data still be useful if it meets the risk threshold ?
  - How much do you trust the entity you are disclosing data to ?

v1.3 - 8

Khaled El Emam –De-identification Methods

## How Many People ?

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- “Journalist” attack – only one record will be re-identified
- In most cases that is enough to cause damage to the organization
- “Marketer” attack – as many records as possible
- Verification cost and intruder objectives plays an important role in deciding whether a “marketer” attack is really feasible

v1.3 - 9

Khaled El Emam –De-identification Methods

## AOL Case

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- In the Summer of 2006 AOL released “anonymized” data on ~20 million discrete search queries for >650,000 individuals on a public web site for researchers to use
- The records include date and time of the query and the web site clicked on, as well as a unique identifier for each user so records can be linked to get a user profile

v1.3 - 10

Khaled El Emam –De-identification Methods

## AOL Users

### Contents

Intro
Ident
Threshold
▶
QIDs
Uniques
Linkage
Tools
End

- #2178: "foods to avoid when breast feeding"
- #3482401: "calorie counting"
- #3505202: "depression and medical leave"

v1.3 - 11  
Khaled El Emam -De-identification Methods

## User #4417749

### Contents

Intro
Ident
Threshold
▶
QIDs
Uniques
Linkage
Tools
End

- "tea for good health"
- "numb fingers", "hand tremors"
- "dry mouth"
- "60 single men"
- "dog that urinates on everything"
- "landscapers in Lilburn, Ga"
- "homes sold in shadow lake subdivision gwinnett county georgia"

v1.3 - 12  
Khaled El Emam -De-identification Methods

## Thelma Arnold

### Contents

Intro
Ident
Threshold
▶
QIDs
Uniques
Linkage
Tools
End



- 62 year old widow living in Lilburn Ga re-identified by the New York Times
- She has three dogs

v1.3 - 13  
Khaled El Emam –De-identification Methods

## What Happened Next ?

### Contents

Intro
Ident
Threshold
▶
QIDs
Uniques
Linkage
Tools
End

- Maureen Govern, CTO of AOL "resigns"
- Abdur Chowdhury, AOL researcher who released the data was fired
- Abdur's boss in the research department was fired
- Big embarrassment for AOL

v1.3 - 14  
Khaled El Emam –De-identification Methods

## GIC Case

### Contents

Intro
Ident
Threshold
▶
QIDs
Uniques
Linkage
Tools
End

- The Group Insurance Commission is responsible for purchasing health insurance for state employees in Massachusetts
- Insurance data on 135,000 state employees and their families was released after being "anonymized"
- Database was matched with the voter list for Cambridge, Massachusetts

v1.3 - 15  
Khaled El Emam –De-identification Methods

## William Weld

### Contents

Intro
Ident
Threshold
▶
QIDs
Uniques
Linkage
Tools
End

- Six people in the database have the same DoB
- Three are men
- One in his 5 digit zip code
- His insurance record was re-identified
- William Weld was the governor of Massachusetts

v1.3 - 16  
Khaled El Emam –De-identification Methods

## Probability of Re-identification - I

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- There is no rational basis for deciding what the threshold probability of re-identification should be

*“whereas to determine whether a person is identifiable account should be taken of all means likely reasonably to be used by the controller or by any other person to identify said person”*

*European Data Protection Directive (95/46/EC)*

v1.3 - 17

Khaled El Emam –De-identification Methods

## Probability of Re-identification - II

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Many healthcare organizations ensure that each record is similar to at least 4 other records (ie, that cell sizes are at least 5)
- This implicitly assumes a threshold risk of 0.2
- There is some justification then, based on precedent, for using 0.2 as an acceptable risk of re-identification

v1.3 - 18

Khaled El Emam –De-identification Methods

## Data Utility

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- There is evidence that distortions to data due to de-identification have a negative impact on analysis
- For example, the power to detect clusters in public health applications is reduced as geographic information is aggregated
- This must be an important factor in any de-identification effort

v1.3 - 19

Khaled El Emam –De-identification Methods

## Trust

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Things to check for:
  - *Good records management practices in place*
  - *Ability to audit*
  - *Data sharing agreement*
  - *Good information security in place*

v1.3 - 20

Khaled El Emam –De-identification Methods



## Quasi-identifiers - I

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Can be used to indirectly re-identify individuals (by making them unique or through linkage), for example:
  - Race, ethnicity, home language
  - Dates (birth, death, admission, discharge, autopsy)
  - Geographical information (residence, proximity to landmarks or unique structures)
  - Diagnostic codes for rare and visible diseases and disorders

v1.3 - 21

Khaled El Emam –De-identification Methods

## Quasi-identifiers - II

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- There may be other quasi-identifiers depending on the particular data set that is of interest
- Inference of quasi-identifiers:
  - Year of birth from graduation year
  - Geographical information from demographics and transactions
  - Gender from names and nicknames
  - Date of death from autopsy date
  - Inclusion of individuals in a longitudinal cohort when only one variable could have changed over time (eg, age)

v1.3 - 22

Khaled El Emam –De-identification Methods





## Uniqueness

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Uniqueness in the Canadian population has received very little study
- We know that  $<0.5\%$  of the population is 90+, therefore this is commonly used as a basis for top-coding
- Consider diagnostic codes for rare and visible diseases and disorders
- Both of the above become risky of geographic information is included in the data to be disclosed

v1.3 - 23

Khaled El Emam –De-identification Methods



## Geography - I

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Full postal codes are as good as identifying information (when coupled with age and gender) because these combinations are unique
- Many residential postal codes have few dwellings, and it is easy to get basic information on the home owners
- This is more difficult and expensive with FSAs, but be careful about FSAs with a small number of residential dwellings (eg, mixed commercial and residential use)

v1.3 - 24

Khaled El Emam –De-identification Methods

## Geography - II

### Contents

- Intro
- Ident
- Threshold
- QIDs
- Uniques
- Linkage
- Tools
- End

- A common way to deal with geographic information is to use population sizes for geographic areas:
  - 20k rule in HIPAA
  - 70k rule used by Statistics Canada
  - 100k rule used by the US Census Bureau
- There are limits to these simple rules because they ignore the number and nature of variables that are disclosed in addition to the geographic information

v1.3 - 25

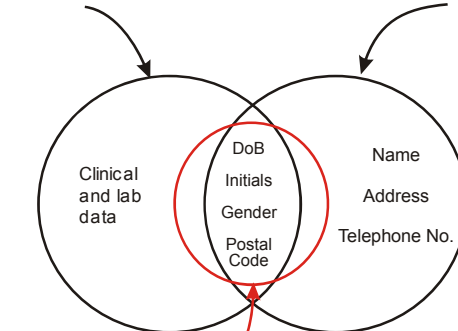
Khaled El Emam –De-identification Methods

## Record Linkage - I

### Contents

- Intro
- Ident
- Threshold
- QIDs
- Uniques
- Linkage
- Tools
- End

Medical Database      Identification Database



Quasi-Identifiers

v1.3 - 26

Khaled El Emam –De-identification Methods

## Record Linkage - II

### Contents

- Intro
- Ident
- Threshold
- QIDs
- Uniques
- Linkage
- Tools
- End

- Vulnerable groups due to record linkage with public sources of information:
  - Professionals whose associations publish a comprehensive list of members (eg, physicians and lawyers)
  - Homeowners
  - Civil servants
- Must also consider non-public sources of information that a potential intruder may have access to

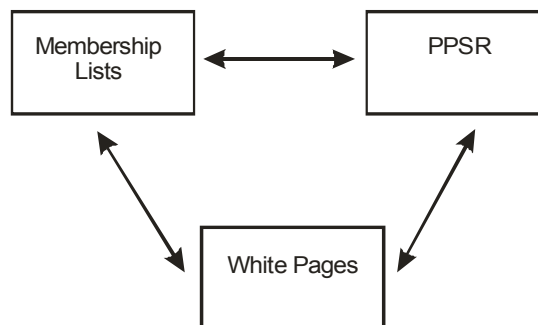
v1.3 - 27  
Khaled El Emam –De-identification Methods

## Professional Groups

We can construct identification databases for specific professional groups

### Contents

- Intro
- Ident
- Threshold
- QIDs
- Uniques
- Linkage
- Tools
- End



v1.3 - 28  
Khaled El Emam –De-identification Methods

## What is the success rate ?

### Contents

- Intro
- Ident
- Threshold
- QIDs
- Uniques
- Linkage
- Tools
- 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/ <b>genderizing</b> LSUC)	100%	100%
• Ability to get initials (source: CPSO/LSUC)	100%	100%

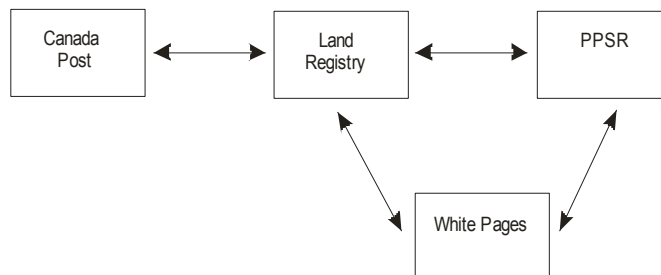
v1.3 - 29  
Khaled El Emam –De-identification Methods

## Homeowners

We can construct identification databases for specific postal codes

### Contents

- Intro
- Ident
- Threshold
- QIDs
- Uniques
- Linkage
- Tools
- End



v1.3 - 30  
Khaled El Emam –De-identification Methods

## What is the success rate ?

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

	Ott	To
• Ability to get initials	93%	100%
• Ability to get DoB	33%	40%
• Ability to get telephone number	80%	50%
• Ability to get gender	87%	95%

v1.3 - 31

Khaled El Emam –De-identification Methods

## Re-id Risk for Homeowners

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- The number of households per postal code is quite small (Ott: 15; To: 20)
- The individuals (homeowners) were unique on common combinations of quasi-identifiers (eg, gender and DoB)
- For these individuals re-identification risk is very high

v1.3 - 32

Khaled El Emam –De-identification Methods

## Civil Servants

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- GEDS is on the Internet: Government Electronic Directory Services
- There are 386,630 individuals in the federal government, GEDS has approx. 170,000 entries
- We selected a sample of 40 individuals in health care related federal departments in Ontario
- Able to get home address for 50%, home telephone number for 40%, gender for 100%, DoB for 22.5%

v1.3 - 33  
Khaled El Emam –De-identification Methods

## Economic Deterrents

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Creating identification files to use for matching using public sources can be quite expensive
- This presents a practical economic deterrent for most users – though plausible it is arguably not very practical
- But there are many re-identification scenarios (insiders) where such an economic deterrent does not exist

v1.3 - 34  
Khaled El Emam –De-identification Methods

## De-identification Tools

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- Most tools that are readily available do not fully automate the process
- De-identification tools need to be risk-based to ensure that the actual re-identification risk is below the threshold
- There is really a risk profile that needs to be managed

v1.3 - 35

Khaled El Emam –De-identification Methods

## Contacts

### Contents

Intro
Ident
Threshold
QIDs
Uniques
Linkage
Tools
End

- eHealth Info Lab:  
<http://www.ehealthinformation.ca/>
- Email:  
[kelemam@uottawa.ca](mailto:kelemam@uottawa.ca)

v1.3 - 36

Khaled El Emam –De-identification Methods

## **Panel 1B: Global Information Flows**

**Chair: Anita Fineberg, Corporate Counsel & Chief Privacy Officer,  
Canada and Latin America, IMS Health Canada**

### **Session Overview:**

This session will focus on privacy and global data flow issues in the context of a case study. The case study will describe a situation involving personal health information being transferred from different entities around the world for the purposes of a multi-national research project. The panel members will discuss the issues raised, consider the current requirements to manage these issues in a privacy-compliant manner and highlight those 'grey' areas of technical compliance that require a risk-based approach to the solutions.

### **Biography of Chair:**

Anita Fineberg is the Corporate Counsel and Chief Privacy Officer for IMS HEALTH Canada and Latin America. She oversees the legal affairs of the company, as well as the management of internal privacy compliance activities and external privacy advocacy and outreach activities. Ms. Fineberg also provides legal and policy advice on privacy matters to IMS' Global Privacy Council in the United States, the European Union, the Asia Pacific Region and Japan.

Ms. Fineberg has worked in the area of privacy and access to information for the past 15 years. Her expertise in the area is rooted in her seven years with the Office of the Information and Privacy Commissioner/Ontario where she held a number of positions including Adjudicator and Legal Counsel.

Prior to joining IMS HEALTH, Ms. Fineberg was counsel to the Ontario Ministry of Health and Long-Term Care, providing advice on the Freedom of Information and Protection of Privacy Act and other legislation administered by the Ministry dealing with privacy and confidentiality. She provided advice on the development of the Ministry's Personal Health Information Protection Act, 2000, as well as the privacy implications of the federal Personal Information Protection and Electronic Documents Act.

Ms. Fineberg is a frequent speaker and course leader on issues related to the privacy of health information. She holds an Honours B.A. in Psychology from Queen's University and an LLB. from the University of Toronto Law School.



## **Biography of Panelist**

### **Adam Kardash, Partner, Heenan Blaikie**

#### **Bio:**

Adam Kardash, a partner at Heenan Blaikie, has been with the firm since 1989. Adam's practice focuses almost exclusively in the information technology and privacy areas. He has worked on a wide variety of transactions involving information technology, including technology acquisitions, licensing, outsourcing and service provider arrangements, and general corporate commercial issues carrying on business over in the Internet and in the electronic environment. Kardash also has extensive experience in the privacy law area, including health privacy, and regularly advises on a broad range of data protection issues and privacy compliance initiatives.

Mr. Kardash is a member of the privacy law, intellectual property, marketing and advertising, and the life sciences and emerging technologies practice groups. He acts for a range of companies in the technology sector, including Canadian subsidiaries of the multinational Internet service providers and technology companies, in addition to servicing the information technology needs of clients of the firm in all industry sectors, including health care, health research, and insurance sectors. On privacy issues, Kardash assists in-house counsel and/or Chief Privacy Officers of a broad range of entities in the private and not-for-profit sectors on conducting privacy impact assessments, privacy and security audits, drafting of privacy policies, privacy compliance systems, and the drafting and negotiation of service provider arrangements involving personal information.

Kardash is a member of the executive of the Privacy Section of the Ontario Bar Association (OBA), and served for three years on the executive of the OBA's Electronic Commerce and Information Technology section. He speaks regularly in the Information Technology and Privacy areas, and for three years taught an MBA course on legal issues relating to electronic commerce at York University's Schulich School of Business. Kardash also sits on the Canadian Marketing Association's Task Force on Interactive Marketing and the eHealth Privacy Committee of the Information Technology Association of Canada.

## **Biography of Panelist**

**Miyo Yamashita, President, Anzen Consulting Inc.**

### **Bio:**

Miyo Yamashita is the President and founding partner of Anzen Consulting Inc. (Anzen), an independent consulting firm specializing in information privacy. Anzen conducts privacy impact assessments and provides privacy consulting services in the areas of privacy risk management, privacy crisis management, privacy policy development and implementation, staff privacy education and training, and privacy best practices relating to the collection, use, and disclosure of personal information. Anzen delivers practical, top-quality, cost-effective privacy solutions in support of its clients' business goals and works with a range of clients, including health care organizations, government, and private industry. Some of Anzen's health care clients include: Canadian Blood Services, Cancer Care Ontario, the Ontario Telemedicine Network, Canada Health Infoway, and the Newfoundland and Labrador Centre for Health Information. Anzen has also provided privacy consulting advice to provincial and territorial Ministries of Health in Ontario and the Northwest Territories, as well as to the City of Toronto. In private industry, Anzen has worked with pharmaceuticals, health information system vendors, and data brokerage companies. Finally, Anzen has also developed a privacy impact assessment template and a privacy training video on the Personal Health Information Protection Act, 2004 for the Information and Privacy Commissioner/Ontario. Prior to beginning Anzen, Miyo served as first the Corporate Privacy Officer at University Health Network (Toronto General Hospital, Toronto Western Hospital, and Princess Margaret Hospital). Miyo has a Ph.D. in communications from McGill University where she specialized in the impact of data protection laws on organizational privacy practices.

## **Session 2A: Medical Identity Theft**

**Chair: Gordon Atherley, Principal, Greyhead Associates**

### **Session Overview**

Identity theft, better termed identity abuse, has emerged as the most serious challenge to electronic health records. The information and communications technology on which electronic health records depend enable identity abuse on a scale unimaginable with paper records. Yet, without accurate identity data, an electronic health record is useless or even dangerous for clinical purposes.

The session will examine current experience relative to the risks of, prevention of, and protection against identity abuse associated with electronic health records. In particular, it will examine implications for healthcare practice, protection of patients, and public policy. It will scan the horizon for technological solutions.

### **Biography of Chair:**

Gordon Atherley holds the British equivalent of the Canadian PhD and MD degrees, and LL.D., Honoris Causa, from Canada's Simon Fraser University. His awards include Officer (Brother) of the Most Venerable Order of The Hospital of St John of Jerusalem, and Fellow of the Royal Society of Arts, UK. His medical specialties are occupational medicine and public health. He is retired from medical practice.

Through Greyhead Associates, of which he is Principal, he provides (a) services as researcher-analyst focused on complex problems on the interface of healthcare, its professionals, and electronic information

systems for healthcare; one such problem is identity abuse (b) expertise in knowledge services and systems involving knowledge bases and knowledge centres for healthcare. He was first President and Chief Executive Officer (rank of Deputy Minister) of the Canadian Centre for Occupational Health and Safety (CCOHS), the Canadian equivalent of the US National Institute of Occupational Safety and Health (NIOSH).

At the time, CCOHS was a federal crown corporation. With its 39-member Board of Governors representing governments, employers and labour in all regions of Canada, during his ten-year tenure he led the creation of Canada's electronic information service in occupational health and safety, and negotiated a groundbreaking information exchange with NIOSH. Knowledge services from CCOHS are now used in some 40 countries.

In academia, he has held senior, tenured, full-time positions, including chair, in university faculties of physics, engineering, and medicine. In Canada, he was full professor, occupational medicine, at the University of Toronto. He is the author of a textbook and has 50 refereed publications in indexed journals.

He is a life member of the Canadian Medical Association and the Ontario Medical Association, and a reviewer for the Canadian Medical Association Journal.



## **Healthcare, Electronic Health Records and Identity-Related Crime**



eHealth Research and Planning



Dr Gordon Atherley\*

\*905 842 9425   [gordon.atherley@greyhead-associates.com](mailto:gordon.atherley@greyhead-associates.com)

## Identity-Related Crime

## Identity-Related Crime, 1

- Identity theft (not yet a criminal offence in Canada)
- Identity-theft-related fraud
- Impersonation for criminal purposes
- Assuming and living a false identity
- Assuming the identity and living the life of another person

## Identity-Related Crime, 2

- Pandemic in scope, facilitated by information technology
- Growing exponentially
- Driven by the value proposition for criminals
- A safer and easier alternative to drug dealing
- Opportunistic

## Identity-Related Crime, 3

- Exploitation of human and technical vulnerabilities
- Inadequately prevented by information technology
- Insufficiently constrained by legislation
- Already operating in healthcare

## Identity-Related Cases

## TJX-Winners as of Oct 07\*

- “According to court documents filed by a group of banks, more than 94 million accounts fell into the hands of criminals as a result of a massive security breach suffered by TJX, the Massachusetts-based retailer”
- “...in this case it is beyond doubt that there is an extremely high risk that the compromised data will be used for illegal purposes,” read the document, filed Tuesday in US District Court in Boston”

\*[http://www.theregister.co.uk/2007/10/24/tjx\\_breach\\_estimate\\_grows/](http://www.theregister.co.uk/2007/10/24/tjx_breach_estimate_grows/)

## TJX, continued

- “Research firms have estimated the total loss from the breach could reach \$1bn once settlements, once legal settlements and lost sales are tallied. But that figure was at least partly based on the belief that fewer than 46 million accounts were intercepted”
- “TJX has taken serious flack for allowing the breach to happen. Last month, Canada's privacy commissioner criticized the company for collecting too much data and using inadequate means of protecting it”

## Salesforce.com as of Nov 07\*

- *Salesforce.com* is an Internet-based Customer Relationship Management application with close to one million users
- Apparently a *Salesforce.com* staffer was tricked by a phish into revealing data that supported a phishing attack on *Salesforce.com*'s customers

\*[http://www.theregister.co.uk/2007/11/07/salesforce\\_phishing\\_scam\\_customer\\_list/](http://www.theregister.co.uk/2007/11/07/salesforce_phishing_scam_customer_list/)

## Identity-Related Criminal Processes



## Identity-Related Crime's Processes

- Harvesting of identity data from electronic and paper records
  - Direct, via staff
  - Indirect, via malware
- Phishing
  - eMail
  - Phone
- Some combination of these
- ? (Identity-Related Criminals are opportunistic)

## Identity-Related Crime's Harm in Healthcare

## Identity-Related Crime Harm in healthcare\*

- Medical error from identity mix-ups
- Robbery and defrauding of patients
- Targeting of people at their most vulnerable time
- Defrauding of payor systems, public and private
- Impairment of trust in healthcare and its personnel
- Liability suits against personnel and organizations
- Unfairness in inequitable access to legal counsel

\*<http://www.taxonmer.com/PublishTxgd001/eHealth,%20Adverse%20Effects,%20International%20Perspectives/index.htm>

## How Healthcare Deals with Risk

## How healthcare deals with risk, 1

- For more than a century healthcare has continuously confronted the contradiction that its most powerful tools are intrinsically dangerous
- At the cost of lives not only of patients, but also of healthcare personnel, healthcare learned that the contradiction *cannot* be resolved by striking a balance between patient care and patient safety

## How healthcare deals with risk, 2

- Healthcare understood that, for the benefits of care to be safely delivered to and trusted by patients, its dangers must be unambiguously acknowledged, rigorously researched and vigorously confronted
- Relative to the concept of *social duty of care*, the law in its various manifestations stipulates what is expected of healthcare and its personnel in acknowledging, researching and confronting the dangers that healthcare brings to patients

## How healthcare deals with risk, 3

- The duties of care are onerous on hospitals and practitioners; the penalties for failures in performance of these duties, significant.
- Individual practitioners, for example, may lose their licences to practice, and therefore their livelihoods
- From time to time, seemingly beneficial technologies, drugs and devices are judged unacceptably dangerous and rigorously regulated or even banned outright.

## How Government Deals with Risk

## Government

- Government is expected to understand that, in driving something that is both powerfully beneficial and intrinsically dangerous, it is called upon in social justice to exercise its obligations to protect citizens against threats over which they have little or no control
- Relative to identity-related crime in healthcare
  - ☐ legislation is neither adequate nor up to date
  - ☐ government is not sufficiently vigorous in regulating itself and its agencies
  - ☐ agencies are not sufficiently engaged with protecting citizens

## Identity-Related Crime Protection and Prevention

And the impact on information  
technology

## Protection for Healthcare, 1

### Healthcare

- Perceives the parallel between Identity-Related Crime and opportunistic and nosocomial infection
- Responds by taking the lead in prevention and protection, in partnership with information technology providers

### Information technology providers

- Understand healthcare's needs
- Respond to healthcare's requirements

## Protection for Healthcare, 2

### Government

- Recognizes that privacy is necessary but insufficient as a basis for legislation
- Upgrades legislation accordingly

### Agencies

- Submit to public-administration norms and expectations equivalent to those applied to healthcare and its personnel

## Vision and mission for healthcare

- In combating the menace of identity-related crime to patients and personnel, healthcare must take the lead and apply the lessons so painfully learned because it is ultimately accountable
- In taking the lead, healthcare will transform information technology in the service of healthcare and perhaps beyond

## **Identity Management in Healthcare**

**Jeff Curtis, Sunnybrook Health Sciences Center**

### **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.



# Identity Management in Healthcare

*Jeff Curtis, Privacy Coordinator*  
Sunnybrook Health Sciences Centre

December 3, 2007



## *Everyone knows who they are (to themselves):*

*Cogito, ergo sum (I think, therefore I am)*  
- Descartes (Discourse on Method, 1637).

*I can, therefore I am*  
- Simone Weil (Philosopher 1909 –1943),

*I think, therefore I am...I think.*  
- George Carlin (Comedian 1937 - )

*I get mail, therefore I am*  
- Dilbert (Timeless)



***Everyone knows who they appear to be (i.e. to the rest of the world):***

***Who you are is a function of:***

What you are: (Caucasian male, 46 yrs, 160lbs., head cold)

What you do: (Privacy Officer, entered by side door)

What you have: (Credit card, money in bank, mortgage)

What you want: (better long distance rates, fewer telemarketing calls)

What you know: (password, too much, not enough, just enough, mother's maiden name...)



***So what's the problem?***

*The problem is:*

*Does anybody else know who you are or believe what you know, have, do, etc.?*



...and will they lend you money? ☺



## Some definitions

- **Identity:** a reference or designation used to distinguish a unique and particular individual, organization or device.
- **Identity Management:** the set of principles, practices, policies, processes and procedures used to realize the desired outcomes related to identity.

→ *Note that who you are becomes inextricably linked with a series of privileges, to the point that....*

*...the privileges can also begin to define who you are.*

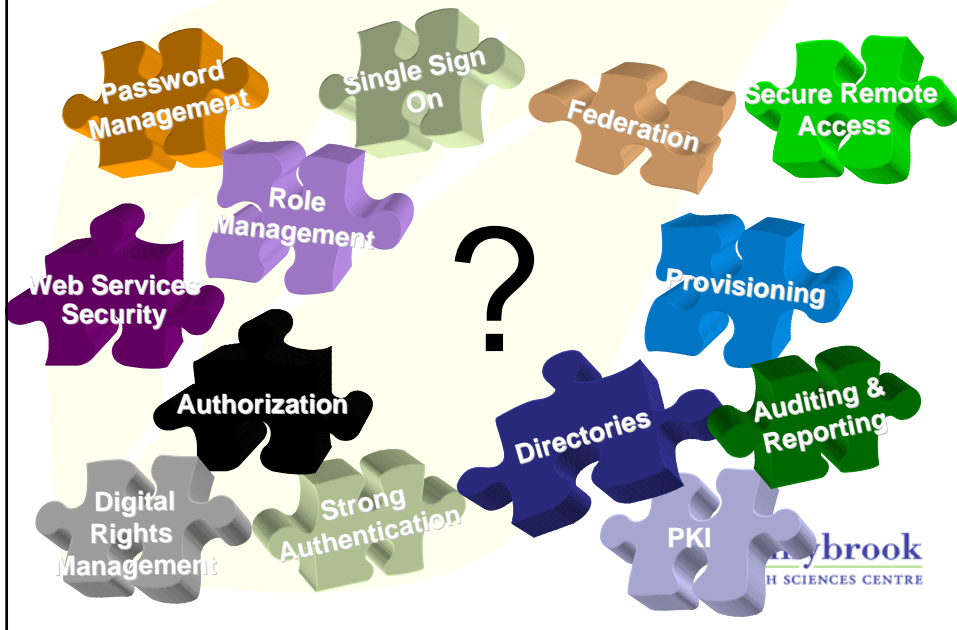
*"I would never want to belong to a club  
that would have me as a member"  
- Groucho Marx*



## Lets get technical...for a moment

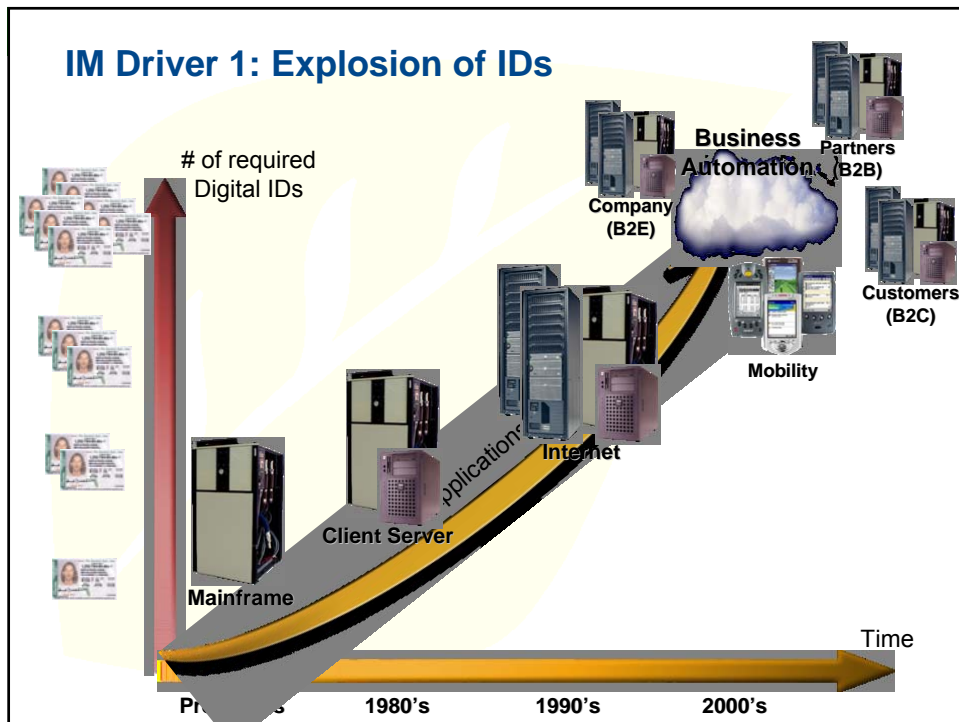
- **Identification:**
  - Collection of untrusted (as yet) information about a subject, such as an identity claim (user ID, your name...your health card number? (see Atherley))
- **Authentication**
  - Verification of a subject's identity by means of relying on a provided claim
- **Authorization**
  - Deciding what actions, rights or privileges can the subject be allowed

## So what's all this have to do with ID Management?




## The problem

- Internet was build so that communications are anonymous
- In-house networks use multiple, often mutually-incompatible, proprietary identity systems
- Users are unwilling to handle multiple identities
- Criminals love to exploit this mess...



### IM Driver 2: IT Security Risk and Compliance

- Rising Tide of Regulation and Compliance**
  - SOX, HIPAA, GLB, Basel II, 21 CFR Part 11, (U.S. but some CDN similarities)...
  - \$15.5 billion spend in 2005 on compliance
- Deeper Line of Business Automation and Integration**
  - One half of all enterprises have Service Oriented Architectures under development – integrates all applications and users
  - “Web services” spending growing 45% CAGR
- Increasing Threat Landscape**
  - Identity theft costs banks and credit card issuers \$1.2 billion in 1 yr
  - \$250 billion lost in 2004 from exposure of confidential info
- Maintenance Costs Dominate IT Budget**
  - On average employees need access to 16 apps and systems
  - Companies spend \$20-30 per user per year for password resets


  
**Sunnybrook**
  
 HEALTH SCIENCES CENTRE

Data Sources: Gartner, AMR Research, IDC, eMarketer, U.S. Department. of Justice

## IM Driver 3: ID Management is...Cool!

[www.barbiegirls.com](http://www.barbiegirls.com)



## IM Driver 3: ID Management is...Cool!

That is: identity Management is now a personal safety issue...and it's also the basis of a customer loyalty program...and it's a brand differentiator...*now how cool is that?*

[www.barbiegirls.com](http://www.barbiegirls.com)



- Pre-teens in Mattel's free [Barbie Girls](http://www.barbiegirls.com) virtual world can chat with their friends online using a feature called **"Secret B Chat"**.
  - Mattel only lets girls "Secret B Chat" with "Best Friends", defined as people they know in real life.
- ➔ *How can Mattel guarantee the identity of the chatter(s)?*

## IM Driver 3: ID Management is...Cool!

### Surprise! You need another Barbie!

- But not just any Barbie...the “relationship” first has to be authenticated by way of the **Barbie Girl**, a \$59.95 MP3 player



#### Meaning:

- It's an RSA token (DUH!), but with cute fashion accessories and snap-on hair styles.
- Tweens now ‘authenticate’ to each other (everybody’s doing it!)

*“...like a PGP key signing party, but with cupcakes”*  
([www.identityblog.com](http://www.identityblog.com))

## IM Driver 3: ID Management is...Cool!

### *“PGP Signing party”? Now that does sound cool!*

**Meaning:** Pink visits Red (in person) and plugs Pink’s ‘key’ into Red’s docking station. Red’s Station records Pink as a ‘known friend’, and Pink’s Barbie records Red as a friend – effectively swapping their respective “public keys”. When Pink or Red wants to chat they can now identify and authenticate each other!



*“Hey – this is Pink...wanna chat?...here’s my ID and your special key that I got when I came over last week, remember?”*

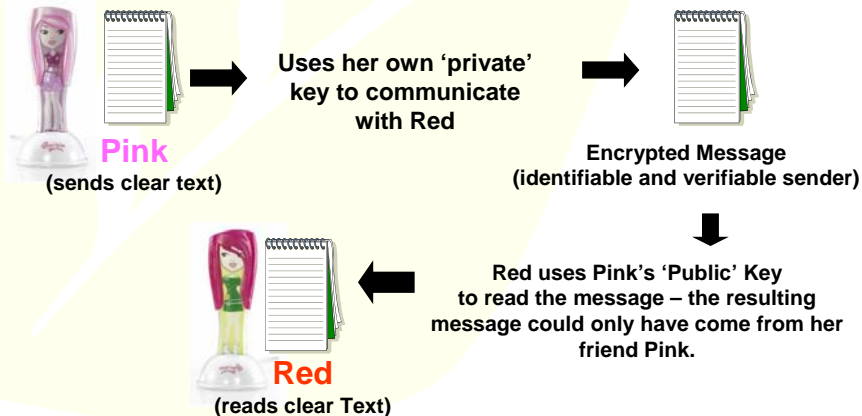


*“Wait a minute I’ll check...yep It’s my special key alright...it must be you...let’s chat!”*



## What's really going on here?

It's a form of **Public Key Cryptography**: Two keys are used for this method: in this case, a private key is used to encrypt. The public key is used to decrypt. Keys are exchanged using trusted networks (cupcake parties, certificate authorities).



## A brief history of Pretty Good Privacy (PGP)

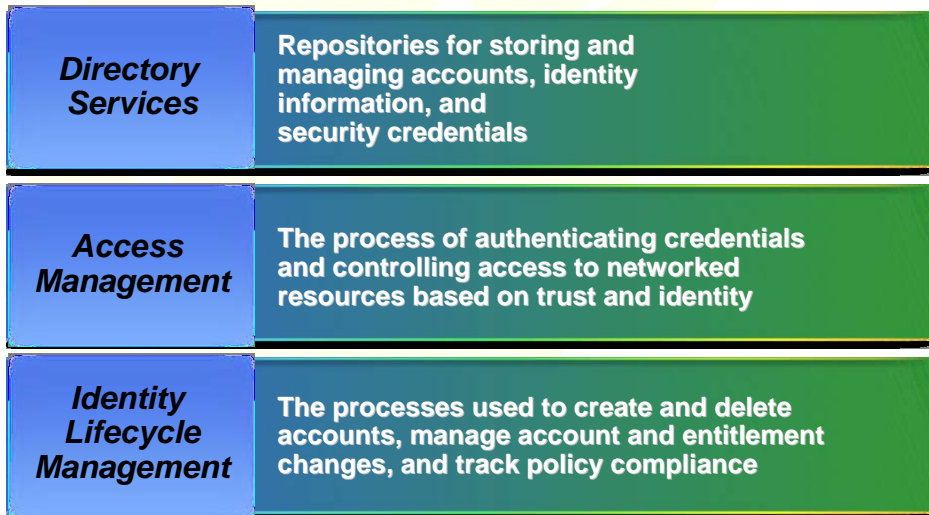
- PGP is a personal high-security cryptographic software application that allows people to exchange messages or files with privacy, authentication, and convenience. PGP can be used to encrypt and digitally sign files and e-mail.
- Developed by Phil Zimmerman in the mid '80s.
- First version released on the Internet in 1991; got immediate NSA attention and encountered legal issues on its use of RSA and Merkle-Hellman cryptography patents.
- Purchased by Network Associates in 1998.

### Why Use it?

- **Privacy** - Store and transmit your data so that only select people may view their contents.
- **Integrity** - Ensure your files, data, and applications have not been modified without your consent.
- **Authentication** - A way to verify that people actually are who they claim to be.

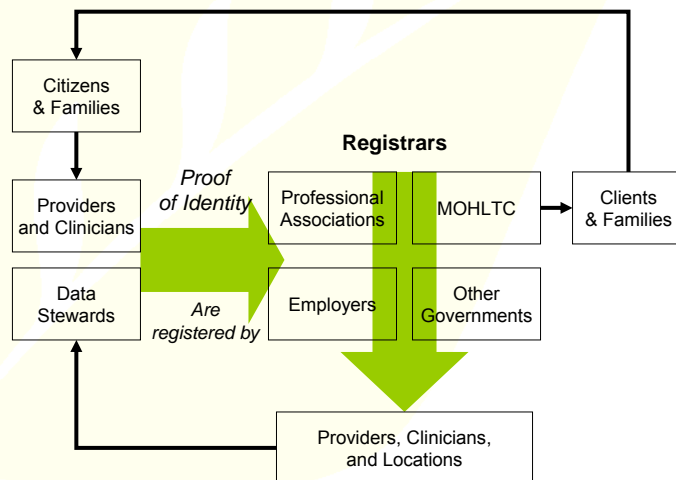


## ID Management in Healthcare - Overview



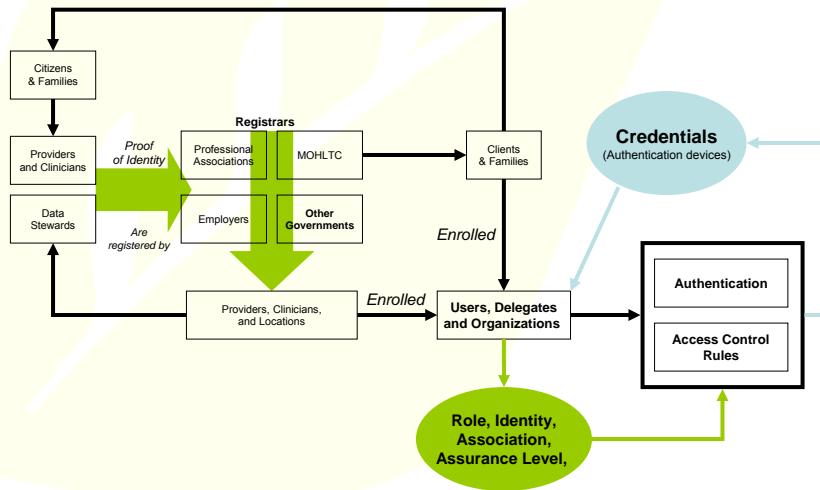
## ID Management in Healthcare

*One version coming to a healthcare network near you*



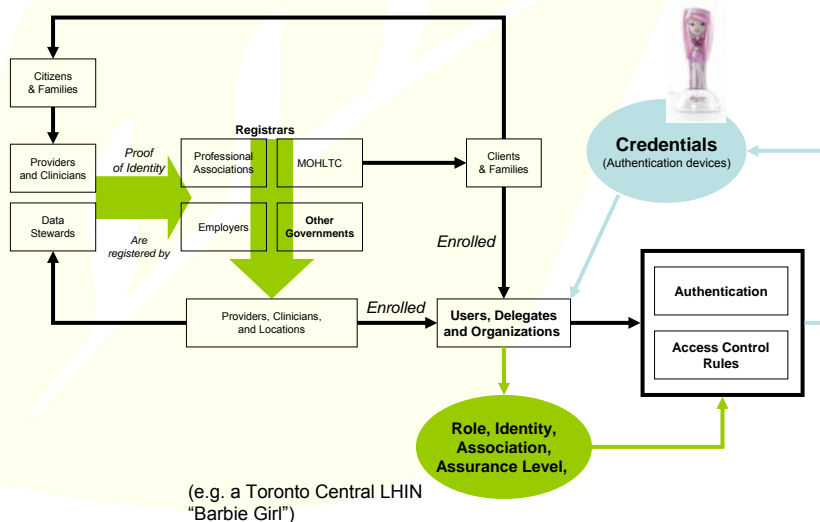
## ID Management in Healthcare

*One version coming to a healthcare network near you*



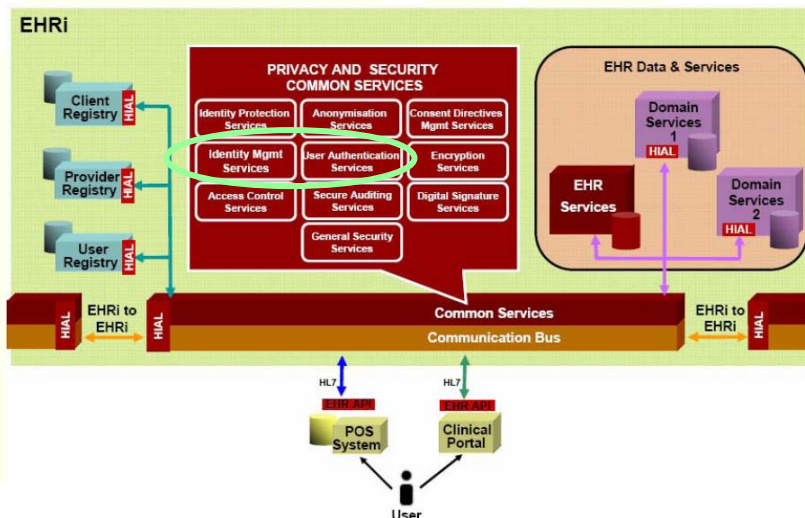
## ID Management in Healthcare

*One version coming to a healthcare network near you*



## ID Management in Healthcare

*Another version coming to a healthcare network near you*



CHI P&S Conceptual Architecture – June 2005

## ID Management in Healthcare



### Identity Management Services

- Includes service components to address the need to accurately identify users of the system.
- Handles tasks such as:
  - registering users
  - **assigning roles that define their access privileges** (e.g. a podiatrist may not be able to access mental health data)
  - managing changes in user status.
- *Users may be patient/persons who have direct online access to portions of their EHR as well as substitute decision makers.*
- *Users may also be systems and applications.*

CHI P&S Conceptual Architecture – June 2005

## ID Management in Healthcare



### User Authentication Services

- A transactional service that builds upon identity management to establish the validity of the claimed identity of a user logging into the system and thereby providing protection against fraudulent transactions.
- In order to manage sessions in which users have access to confidential information, authentication tokens are generated with protective characters such as user ID and time-out

CHI P&S Conceptual Architecture – June 2005

## ID Management in Healthcare - Challenges

- Not all patients or all users are identifiable within the 'system'—where's the registry?...who's the registrar?...is it up to date?...
- Not all systems are subscribers to a single central registry – reliably resolving unique identities across the province in the short to medium term will be difficult.
- Can a user (patient) opt out of system registration:
  - i.e. can they choose to not be registered and still receive services?
  - what would be the effect on the electronic health record of scaled non-registration – e.g. say, 20% non-participation in an EHR?
- Shared systems are beginning to rely on both patient and user registries – the time for ID 'rationalization' is now.
- 'Better' ID management costs more time and money:
  - How much ID management is enough?
  - Technical and administration challenges will continue

## ***Thank You***

**Sunnybrook Health Sciences Centre  
Privacy Office – [privacy@sunnybrook.ca](mailto:privacy@sunnybrook.ca)**

**[jeff.curtis@sunnybrook.ca](mailto:jeff.curtis@sunnybrook.ca)  
(416) 480-6100 ext. 3538**

**Public info at [www.sunnybrook.ca](http://www.sunnybrook.ca)  
“Patient’s and Visitors” > “Privacy and  
Confidentiality”**

## **Medical Identity Theft**

### **Neil Stuart, Partner, IBM Global Business Services**

#### **Bio:**

Neil Stuart is a practice leader in IBM Global Business Services' health care consulting practice. Prior to the formation of this consulting group in IBM, Neil was a Partner with PricewaterhouseCoopers. He also has a status-only appointment in the University of Toronto's Faculty of Medicine. Neil holds a Ph.D. from Brandeis University where he was a fellow in the University's Health Policy Centre.

Neil's consulting work focuses on health services restructuring and strategic change in health care organizations. He was an author of Healthcare 2015 – Win-win or Lose-lose, a study that looks at the future of health care and how it must transform to respond to the challenges of the coming decade.

Neil has served on the editorial board of the Healthcare Management Forum. Neil also taught for several years in the University of Ottawa's Masters of Health Administration program and is the author of many published journal articles and conference presentations on health care and social issues.

Neil has led and participated in numerous high profile consulting assignments including a review of the lessons learned from Ontario's experience with SARS. Neil helped facilitate the development of the Health Information Roadmap, a national agenda for health information in Canada. His team conducted an evaluation of seven pilot programs for primary care reform in Ontario. He was also engaged in the planning of a new medical school in Northern Ontario.

Neil serves on the Board of Toronto East General Hospital.

He is a Certified Management Consultant (CMC).



IBM Global Business Services

## *Electronic Health Information and Privacy Conference*

### *Medical Identity Theft*

Neil Stuart, IBM Global Business Services

Ottawa, December 3, 2007



[www.ibm.com/healthcare/ca](http://www.ibm.com/healthcare/ca)

© Copyright IBM Corporation 2007

Not for external circulation

IBM Global Business Services



## Overview

- My perspective:
  - as a hospital board member
  - as a consultant with a large technology and technology services company
- What is the risk?
- The role of hospital boards
- What technology firms can offer to address risks

## Health information risks

- There are a number of different types of risk that arise with health information and electronic health information:
  - **Privacy** - - the inappropriate disclosure of personal health information
  - **Authentication and authorization** - - invalid identification of patients or providers who seek entry to a health information system and related risks around controlling access to individuals' information within those systems
  - **Integrity issues** - - errors or inaccuracies that could give rise to patient safety issues, or to unfounded type casting or embarrassment of patients
  - **Fraud** - - intentional misuse of health information by a provider or user
- 'Identity theft' describes instances where parties masquerade as an eligible patient or as an authorized care provider or family member, a threat that gives rise to or contributes to the more general risks above

## Dealing with identity theft as one potential threat

- Identity theft is one of many potential threats and it is difficult to fully anticipate all the forms it might take
- **It does not make sense to develop an architecture and policy framework just to deal with identity theft alone. Rather it should be addressed in the context of a broader privacy and security architecture.** And this needs to be built around key principles that address the range of broader risks



## Identity theft as a threat

- Identity theft can take several forms:
  - Individuals masquerading as others to get access to 'covered care'
  - Individuals masquerading as others to avoid stigmatizing diagnoses or interventions appearing in their records - - potentially resulting in incorrect attribution of diagnoses or treatments
  - Providers using identities to submit fraudulent claims
  - Unqualified individuals masquerading as providers to practice illegally or make illegal orders/prescriptions
- Identity theft can lead to inaccuracies in individuals' health information and this in turn can result in significant patient safety risks - - e.g. invalid blood typing
- **Because of the public nature of health care coverage in Canada, the issue of identity theft for financial gain has been much less of a concern here than in the U.S**

## Identity theft as a threat (continued)

- Medical identity theft is not a threat unique to *electronic* health records. **EHRs actually hold the potential to better control identity theft:**
  - Through improved opportunities for authentication
  - Through better opportunities to track unusual or spikes in individual use, as is done with credit card use
  - Through easier or automated consistency checks and controls
- EHRs also provide unique opportunities to identify providers who abuse their access to personal health information by accessing information that is not directly related to their care-giving responsibilities

## Identity theft as a threat (continued)

- Health information risks, and particularly the threat of identity theft, can be significantly reduced by **giving the patient themselves greater access and recourse**:
  - Giving individuals access to their health records
  - Enabling them to seek quick correction of any inaccuracies/errors in their health information
  - Letting them know who has accessed their health records
- Connecting the consumer/patient to their health information could help to reduce any anxiety about their health information. It will make the information transparent to the consumer/patient, will help validate the information and will build trust

## Identity theft as a threat (continued)

- Misuse of personal health information can also be reduced with **systems of internal controls**. Experience in the financial services sector shows you do not have to understand or foresee all the specific threats to identify controls that will minimize threats like phishing or web site spoofing
- When we look at the different forms identity theft can take, indeed when we look at broader health information risks, they can be rooted in either:
  - the **actual technology** and weaknesses in its design, or
  - the **way the technology is used**
- In the health care sector, the **complexity of the sector** and the **complex nature of health information** itself make the latter category of risk a particular concern. The next three slides provide elaborate on this point

## What is the risk? Health care is different

- Information risks in health care are very different from the risks in other business sectors e.g. financial services
- Risks of inappropriate disclosure of **sensitive personal health information** (e.g. mental health conditions, addictions, STDs, abortion, genetic information) are **associated more with personal harm than financial harm**
- In health care there is a very **wide range of potential users** with access to health information - - provincial ministries/departments, health regions/LHINs, hospitals, clinics, independent labs, physician offices, insurers, health call centres, etc. They can span public and private sectors - - and often they are covered by different privacy legislation. And the scale can be very different - - a health region covering a million people approaches privacy and security very differently from a physician's office. And within these organizations there can be a range of players accessing the information - - clinicians, unit clerks, health records staff, planners, researchers, etc

## What is the risk? Health care is different (continued)

- There are complexities around managing and authenticating access to information - - it needs to be **context specific**. i.e. in what capacity is an information user accessing information
- And complexities with access authorization by non-medical individuals other than the patient e.g. relatives and people acting on behalf of the patient. There are unique data access issues with children once they reach age of majority and a parent cannot access without consent

## What is the risk? Health care is different (continued)

- **Health care is increasingly networked and team-based** which means a significant increase in the sharing of personal health information, whether it is done electronically or not
- **New channels of health care delivery** are being introduced - - e.g. telehealth, health call centres, patient portals, retail health care, web services, etc.
- There is a shift in emphasis from short-term, episodic acute care to ongoing management of **chronic conditions and chronic diseases**, life-long care and this adds emphasis to maintaining and continuously sharing health information
- So, unlike other business sectors, personal information in health care will often remain on individuals' records for their **life time** or even beyond
- The **EHR is generally not a singular record** but rather the product of linking a number of sources of personal health information
- **EHR initiatives are still a 'work in progress'**, and will continue to evolve and become more complex and comprehensive in the years ahead, with increasing degrees of patient involvement in the records. Thus the risks will also evolve and become more complex. **Managing risks is not a one-shot deal!**

11

[www.ibm.com/healthcare/ca](http://www.ibm.com/healthcare/ca)

© Copyright IBM Corporation 2007

## The Paradox of e-Health

- **Our health care leadership, political decision makers and even the media push for e-Health**, and say they cannot get it fast enough
- They want it for:
  - Greater patient safety
  - Elimination of redundancy
  - Improved service/access
  - Streamlining/improving care processes
  - Integrating providers/services
  - Giving patients/users more control, the opportunity for more self-service and a better patient experience
- According to the Ontario Health Quality Council, 32,000 Ontario patients are made worse each year because of **errors caused by the lack of electronic health records**
- But, we have concerns about the risks. **Patient safety and privacy are among the goals of e-health, but they also rank among the risks of e-health**

12

[www.ibm.com/healthcare/ca](http://www.ibm.com/healthcare/ca)

© Copyright IBM Corporation 2007

## The Paradox of e-Health (continued)

- **'Interoperability'** (or the ability to share health information among providers) is a goal of many e-health initiatives
- Integrated health care delivery, team-based care and patient engagement are three of the highest priorities for health reform -- and they all call for sharing of individuals' health information
- **And yet it is this very goal of interoperability that raises so many of the concerns about risks!**
- As we explore measures/controls to reduce these risks, we need also to recognize the **risks of constraining interoperability**. If providers cannot share data electronically, work-arounds will proliferate -- paper copies and CDs being made and shared, faxes, etc
- These work-arounds will generally carry much greater risk and be harder to monitor and control
- **Our challenge is to, at the same time, minimize risks and maximize benefits**

## Hospital board perspective

- Boards have responsibility for appointing CEOs and oversight of hospital management and medical staffs
- And they have ultimate responsibility for ensuring the hospital's compliance with relevant legislation, including privacy legislation (e.g. PHIPA, Ontario 2004)
- Boards have fiduciary responsibility to see that hospitals have appropriate risk analysis and risk management
  - Patient safety
  - Technology
  - Financial
  - Organizational reputation
  - Privacy
- Under PHIPA, **hospitals are 'custodians'** of extensive personal health information. But as custodians there remain **obligations to share information** appropriately

## How hospital boards approach their responsibilities

- **Boards ask questions and request information/briefings from hospital leadership and they seek assurance that risks are being addressed. To do this effectively boards need to either have individuals among their members who are qualified to ask the right questions or they will need to engage independent advisors/auditors**
- Boards monitor the performance of hospital CEOs and chiefs of medical staff -
  - goal setting, annual assessments and compensation
- They monitor hospital performance - - score cards that address a range of areas from patient safety and patient satisfaction to financial performance
- Commonly, Ontario hospital boards receive briefings on privacy and information security, often through one of their committees e.g. a quality committee or risk management committee
- They also receive the results of external review processes, e.g. external audits, hospital accreditation surveys, etc

## Technology firm perspective

- Technology firms are about offering effective solutions to solve critical industry problems - - e.g. protecting privacy and addressing the threat of identity theft
- They offer a range of technology solutions and services that help to protect sensitive data and help health care organizations manage health information more appropriately. The latter is done through designing better work processes and checks and balances for better health information management
- Areas of assistance include:
  - **Consulting services** to help: identify and implement best practices; analyze risks and develop risk management practices; design and implement structures, policies and governance for effective privacy and security; create awareness and adoption of appropriate behaviours/processes; conduct compliance assessments
  - **Designing, implementing and in some instances even operating systems** to facilitate privacy and security e.g. identity and authentication management, access control, encryption, etc

## Technology firm perspective (continued)

- The leading firms will also take a holistic view of the issue (not just advocating point technical solutions). They will take **a data-centric security perspective** vs. an enterprise-centric perspective - - **addressing the 'content' as well as the 'container'**. This is key for health care where all the data generally does not belong to a single enterprise
- Health care organizations usually have a good grasp of clinical risk. They have much less experience of **how IT introduces additional risks**. And this is where technology firms can bring in their experience and expertise, address the relationships between business processes and technology, share best practices, and draw on other industry sectors
- Given health care's relatively late entry into the e-world, there are **opportunities to leapfrog other sectors**. e.g. taking advantage of biometrics

## Root causes: the 'content' as well as the 'container'

- **Security failures (Safeguards)**
  - Systems hacked into
  - Physical security breached
- **Not feeling responsible for protecting data (Accountability)**
  - Records left on desks at night
  - Backup tapes left on a loading dock
  - Records not disposed of securely
  - Leaving sensitive info in the printer - - print accountability
- **Having data you shouldn't have (Limited Collection/Retention)**
  - (Or data that is more sensitive than it needs to be)
  - Laptops with personal information on them
  - Keeping data longer than necessary
- **Improper use of data (Focus on Purpose)**
  - A health care worker looks up the record of a neighbour
  - Acknowledgement of appropriate context for access

*From  
Nigel Brown, IBM, 2007*

## Minimizing the 'value proposition' for identity theft in health care

- Dr. Atherley argues persuasively that medical identity theft is and will be driven by **the value proposition for the theft**. That this centres overwhelmingly on the value of information which might be found in patient records that either gives opportunity for financial fraud (e.g. bank account or credit card information) or personal and family information that enables theft of identities for broader purposes
- This takes us back to the central importance of Nigel Brown's point about limiting the collection and retention of information that is not essential. **The importance of clarity around purpose and focus of information collection/retention**. The importance of minimizing information that is high value for identity theft, and where such information is required, managing the risks effectively
- Interestingly, the story from the UK 10 days ago of the **loss of sensitive personal information on 25 million Britons** is providing lots of ammunition to those in the UK who were asking why the new identity cards that the British government is proposing have to contain so much information, much more information than is contained in any identity card introduced in other European countries

19

[www.ibm.com/healthcare/ca](http://www.ibm.com/healthcare/ca)

© Copyright IBM Corporation 2007

## Resources/tools

- The Ontario Hospital Association, the Ontario Medical Association and the Information and Privacy Commissioner of Ontario prepared **Health Information Privacy Toolkits** to help hospitals and physicians achieve compliance with the 2004 PHIPA legislation
- Ontario's Smart Systems for Health (SSHA) has **online training on both privacy and security** to help providers comply with Ontario's PHIPA and SSHA is currently collaborating with some hospitals on further initiatives in this area
- COACH - - Canada's Health Informatics Association published a new set of **'Guidelines for the Protection of Health Information'** in March 2007
- Canada Health Infoway has developed a **Privacy and Security Architecture for EHRs**
- The Canadian Standards Association's **Privacy Principles**

20

[www.ibm.com/healthcare/ca](http://www.ibm.com/healthcare/ca)

© Copyright IBM Corporation 2007



## Infoway's Privacy and Security Architecture for EHRs

It identifies 10 privacy and security services

1. a **User Identity Management Service**
2. a **User Authentication Service**
3. an **Access Control Service**
4. a **Consent Directives Management Service**
5. an **Identity Protection Service**
6. an **Anonymisation Service**
7. an **Encryption Service**
8. a **Digital Signature Service**
9. a **Secure Audit Service**
10. **General Security Services**



<http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf>

## The CSA's Privacy Principles



- |                 |   |  |   |
|-----------------|---|--|---|
| Enterprise Wide | { | 1. Accountability                                    | ▪ Set internal rules and how we make sure we follow them                    |
|                 |   | 2. Openness  | ▪ Communicate accountability measures externally to foster trust/confidence |
| Transactional   | { | 3. Identifying Purposes                              | ▪ Set client expectations and make commitments                              |
|                 |   | 4. Consent   | ▪ Negotiate with client as appropriate                                      |
|                 |   | 5. Limited Collection (Limited Sensitivity/Identity) | ▪ Reduce Liability  |
|                 |   | 6. Accuracy  | ▪ Ensure quality  |
|                 |   | 7. Limited Use, Disclosure, Retention                | ▪ Follow the rules and specific commitments                                 |
|                 |   | 8. Safeguards  | ▪ Protect the data  |
| Client Support  | { | 9. Individual Access                                 | ▪ Give clients the ability to check status/relationship                     |
|                 |   | 10. Challenging Compliance                           | ▪ Detect and address client satisfaction issues                             |

## Some best practices outside Ontario



- Vancouver Coastal Health (VCH) has developed a **Privacy and Information Governance Structure**
- VCH has a **Regional Information Privacy and Confidentiality Policy** and has created a centralized **Information Privacy Office**
- VCH also developed a **privacy/security education toolkit** designed for physicians and they can get CME credits for following it

## Wrap

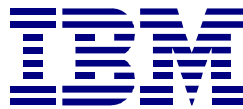
- The challenge is to optimize the benefits and manage the risks
- This is a challenge faced with most significant innovation - - new forms of commerce, new forms of transportation, new energy sources, new therapies, new channels of service delivery, new forms of access and even self service
- **EHRs are a dynamic, evolving field. New forms of service delivery are continually being introduced. We must continue to analyze emerging risks and address them on an ongoing basis.** We have to continue to educate stakeholders of the evolving risks
- And **we must ensure flexibility** to refine and develop new approaches to managing risk as our understanding of the risks evolves - - this is new ground and we will not be able to foresee the nature and significance of every risk - - above all **we have to be able to learn and adapt**
- We need common, accepted definitions of health IT risks and clarification of standard risk management objectives and protection principles
- **We have to make sure that people on the front line, who ultimately have to make the EHR work, have tools and practices they can use. Let's not paralyze them with a morass of controls**

## Contact info

---

- Neil Stuart  
[neil.stuart@ca.ibm.com](mailto:neil.stuart@ca.ibm.com)
- Nigel Brown  
[nigel@ca.ibm.com](mailto:nigel@ca.ibm.com)
- Paul Wing  
[paulwing@ca.ibm.com](mailto:paulwing@ca.ibm.com)

Visit IBM health care at: [www.ibm.com/healthcare/ca](http://www.ibm.com/healthcare/ca)



## **Session 2B: Who's Responsible? Governance and the iEHR**

### **Joan Roch, Chief Privacy Strategist, Canada Health Infoway**

#### **Session overview:**

Who gets access to the EHR? What do they get access to? Who will make these decisions? These are just a few of the questions that people ask as the EHR initiative moves forward. They are questions related to overall governance of the EHR.

Earlier this year, Canada Health Infoway released a White Paper on Information Governance. This session will draw from that work to illustrate elements of governance that are unique to the EHR environment. The session will also feature representatives

#### **Biography of Chair:**

As Chief Privacy Strategist at Canada Health Infoway Ms. Roch is responsible for ensuring that privacy is being addressed by Infoway in its overall program to accelerate the development of a pan-Canadian system for electronic health records.

Roch has over 30 years experience in program policy and information management and for the last 10 years has focused on health information and privacy. She was the first Chief Privacy Officer for the Canadian Institute for Health Information (CIHI). Under her guidance the Privacy Program at CIHI grew to be widely respected and regarded as the model to be followed.

Roch has developed privacy training programs, provided advice on incorporating privacy enhancing practices into system developments and prepared submissions to special federal and provincial review and legislative committees on health information and privacy. She has also co-authored numerous privacy impact assessments on systems and programs of varying size and complexity.

Contributions were made by Roch to the development of the Ontario Hospital Association Privacy Tool Kit and the COACH (Canada's Health Informatics Association) Guidelines for the Protection of Personal Health Information – 2004. She was a member of the Advisory Committee on Infrastructure and Emerging Technology's Protection of Personal Health Information Federal/Provincial/Territorial Working Group that prepared the Pan-Canadian Health Information Privacy and Confidentiality Framework; the Canadian Institutes for Health Research Privacy Advisory Committee that produced the Best Practices Guidelines for Researchers and has sat on Steering Committees for privacy research projects.

Roch has provided practical privacy advice to national and provincial health organizations and has spoken at many conferences, local, national and international, on privacy impact assessments, building privacy programs, building privacy audit programs and privacy issues facing health organizations and researchers. She is currently focusing on the broader topic of information governance in the context of the electronic health record. of jurisdictions in the midst of addressing EHR governance. They will share their experiences and strategies for moving governance discussions forward and for establishing mechanisms to address EHR governance issues in their jurisdictions.



## Who's Responsible? Governance in the iEHR

2007 Electronic Health Information and Privacy Conference  
Ottawa, Canada - December 3, 2007

**Joan Roch, Chief Privacy Strategist, Canada Health Infoway**

Creating Healthy Connections

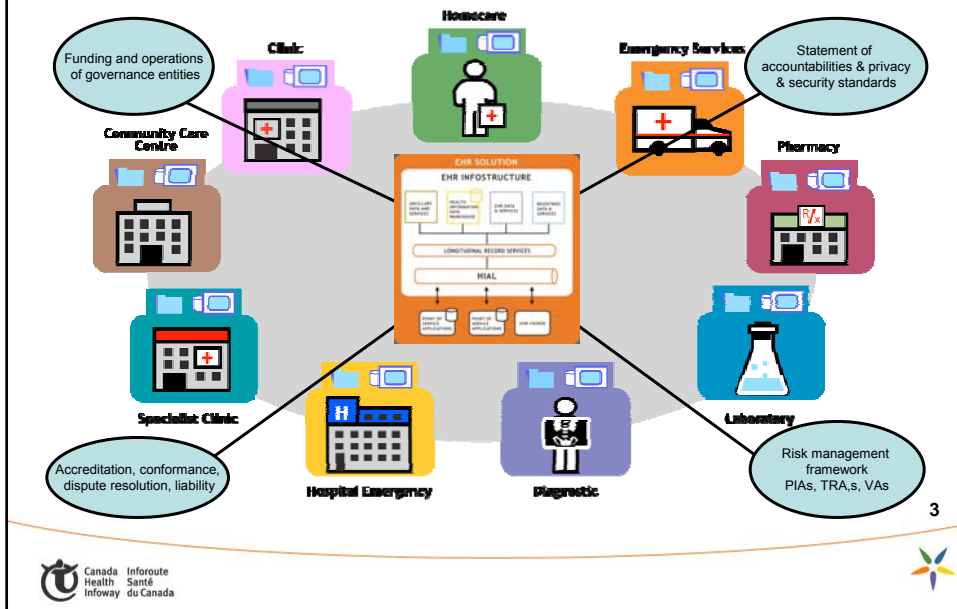
## Outline for today's session

- An overview:
  - the EHR initiative
  - governance and the EHR
  - the Privacy Forum
- What Canadians Think – 2007
  - Mary Lysyk
- Showcase 1 – Newfoundland and Labrador
  - Lucy McDonald
- Showcase 2 - British Columbia
  - John Cheung & Bill Trott

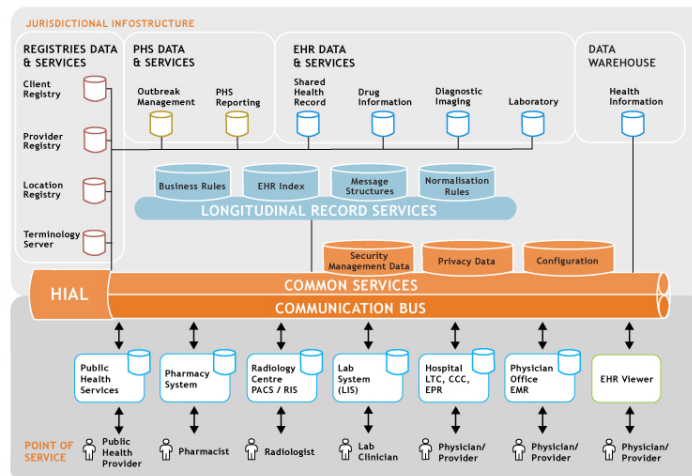
2



## The vision



## EHR architecture





# The Vision

*An electronic health record ( EHR) is a secure and private lifetime record of an individual's health and care history, available electronically to authorized health providers.*

*It facilitates the sharing of data –*  
***across the continuum of care, across health care delivery organizations and across geographies.***

5

 Canada Inforoute  
Health Santé  
Inforoute du Canada



# Sample of an EHR

**Results and images**

**Patient information**

**Medical alerts**

**Medication history**

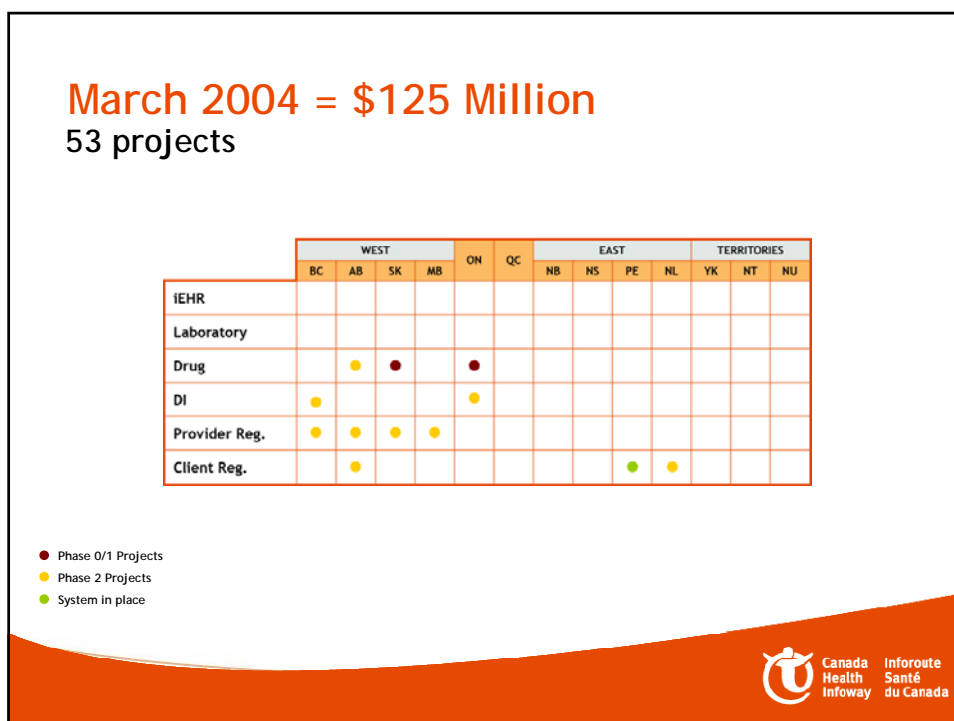
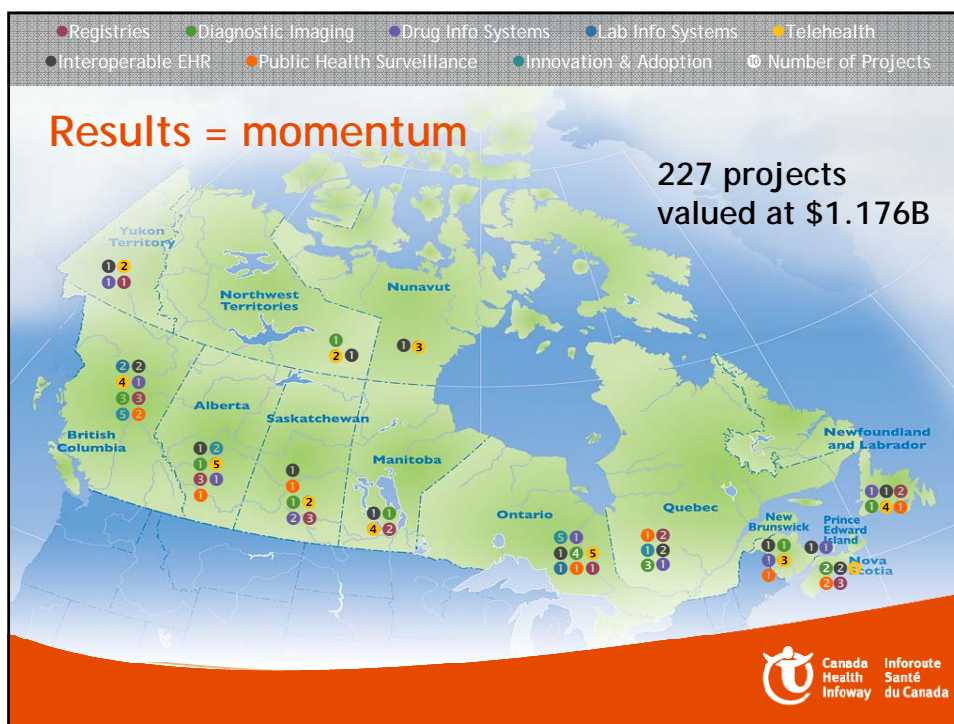
**Interactions**

**Problem list**

**Immunizations**

**Canada Inforoute  
Health Santé  
Infoway du Canada**

**6**





**March 2007 = \$1.176 B**

227 projects

	WEST					QC	EAST				TERRITORIES		
	BC	AB	SK	MB	ON		NB	NS	PE	NL	YK	NT	NU
IEHR	●	●●	●	●	●	●	●	●	●	●	●	●	●
Laboratory	●	●	●		●	●	●	●	●	●		●	
Drug	●	●	●	●	●	●			●	●	●		
DI	●●	●	●	●	●●	●●	●	●	●	●		●	
Provider Reg.	●	●	●	●		●	●	●		●			
Client Reg.	●	●●	●	●	●	●	●	●	●	●	●	●	
Public health	●	●		●	●	●	●	●	●	●	●	●	

● Phase 0/1 Projects

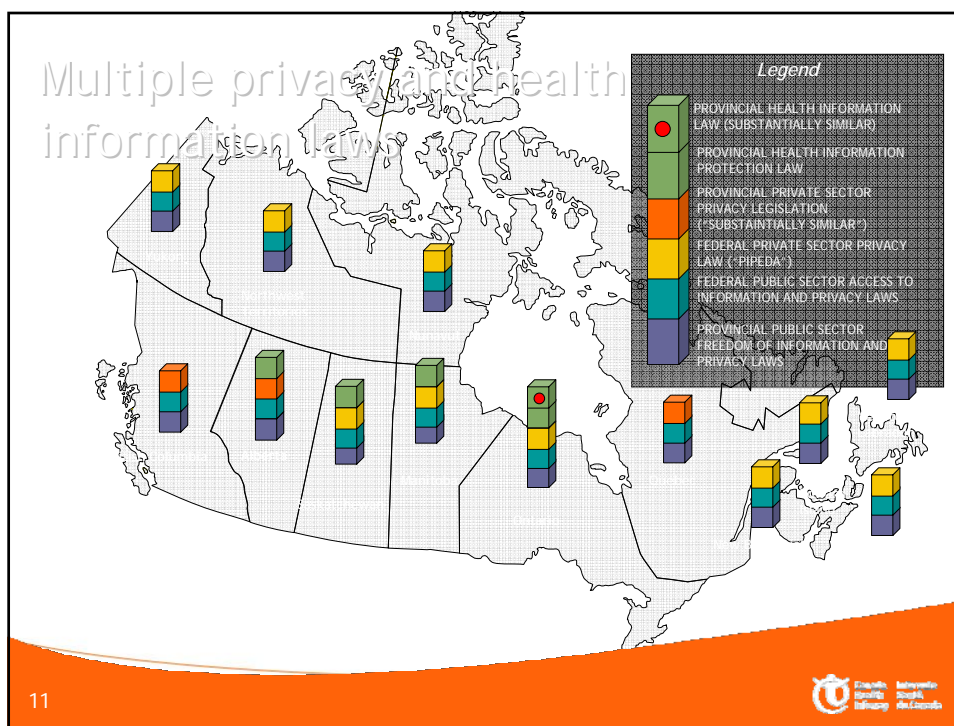
● Phase 2 Projects

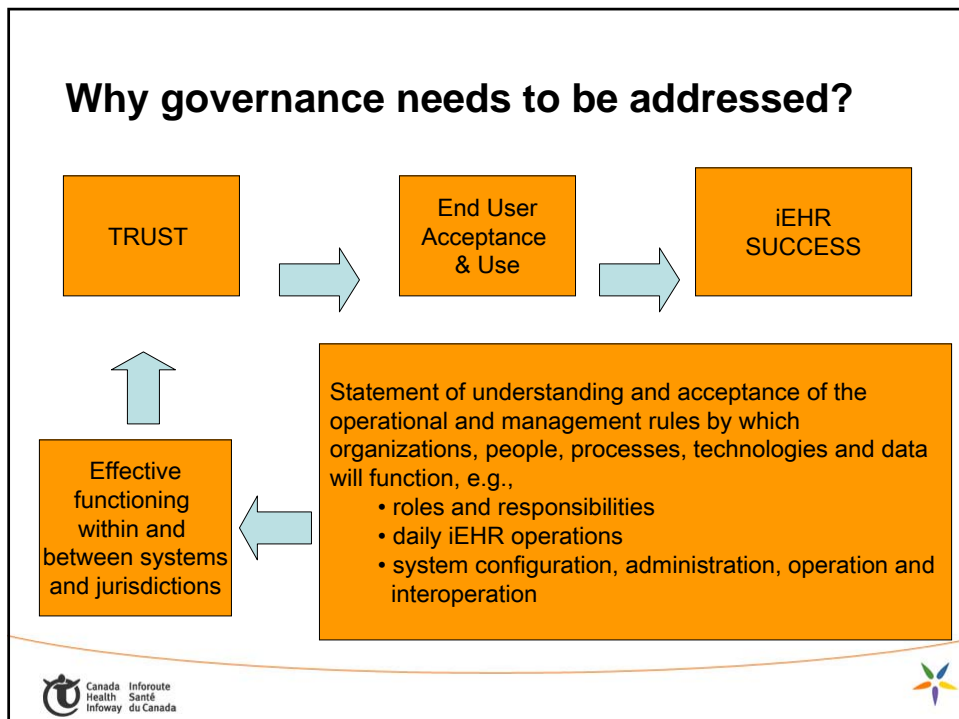
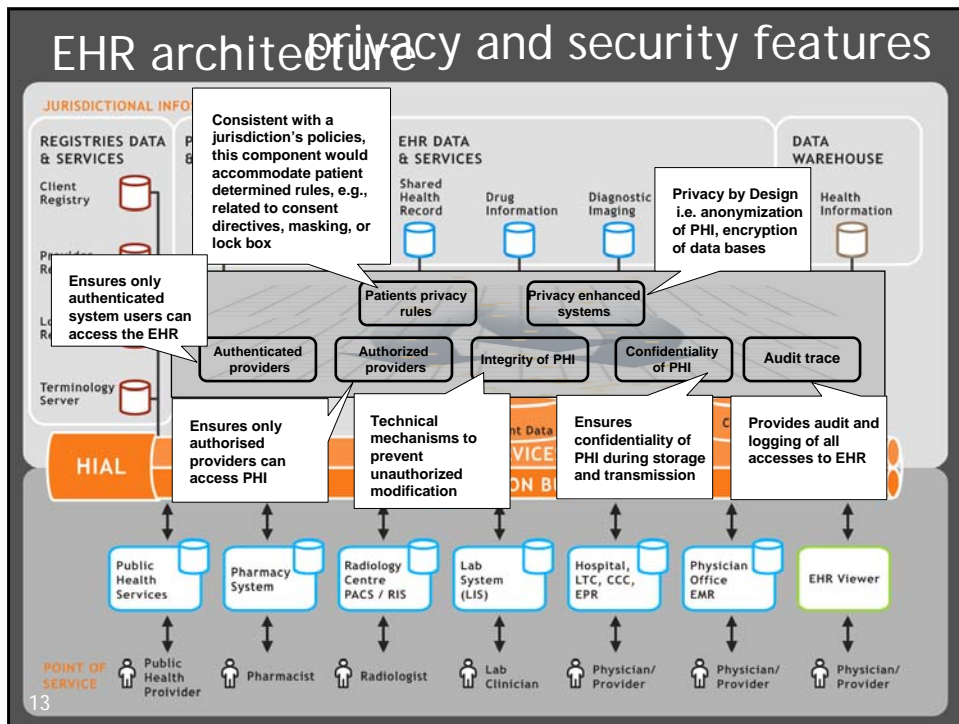
● System in place

## Strong support for the EHR continues

• In 2007 Infoway joined with the Office of the Privacy Commissioner for Canada and Health Canada, to update the previous surveys. Initial findings show:

- An increase in the public's support for, and comfort with, the EHR:
  - 2003 85% support EHR
  - 2007 90% support EHR
- The 2007 survey also asked about people's experience with the EHR
  - 30% have had some interaction
  - This group was even more supportive of the EHR and its benefits
- Canadians continue to indicate that a number of measures would increase their confidence and comfort with the EHR, including sanctions for inappropriately using the information





## ***The White Paper on Information Governance***

- Highlighted 'information governance' topics requiring attention in the iEHR context
- Key Objective:
  - stimulate thought and action
- Reaction:
  - support for further work on the topics
- Follow – on action:
  - creation of the Privacy Forum

15



## **The White Paper on Information Governance - Key Messages**

1. Information governance matters become more important as we move towards implementation of EHRs both within and across jurisdictions.
2. Information governance issues are already present in the paper world. Their effect becomes more apparent in the EHR context.
3. Addressing the topics is a process and will occur over time.
4. Solutions will ultimately be driven by the jurisdiction's legislation and health delivery structure.
5. An overall EHR governance structure needs to be addressed to support effective operation of the EHR system within and across jurisdictions.

16



## Governance – what is new in the EHR context

- The shared health record. The EHR is 'access' based as opposed to 'disclosure' based.
- The EHR environment requires a new trust arrangement.
- The EHR forces co-ordination and the articulation of rules not previously articulated. e.g. access rules.
- The EHR increases the visibility of actions. E.g., audit trails.
- The EHR increases the likelihood of inter-jurisdictional flow of data.
- The EHR highlights privacy requirements.

17



## Information governance topics identified in the White Paper

Topic	Present in both paper and EHR contexts	New
1. Accountability	X	
2. Openness	X	
3. Information custodianship	X	
4. Trans-border data flow	X	
5. Information notices	X	
6. Information consent	X	
7. Limiting collection	X	
8. Limiting disclosure	X	
9. Secondary use	X	
10. Patient access	X	
11. Accuracy and data quality	X	
12. Data retention, archiving & disposal	X	

18



## Information governance topics identified in the White Paper

Topic	Present in both paper and EHR contexts	NEW
13. Auditing and security incident handling	X	
14. Risk assessment		X
15. Compliance mechanisms		X
16. Liability and sanctions	X	
17. Assessment of information governance	X	
18. Access controls		X
19. Electronic signatures		X
20. User identity management		X
21. Privacy of communities of interest	X	

19



## The Privacy Forum



- Launched November 2007
- Unique composition:
  - Includes a representative from each Health Ministry and each Privacy Commissioner/Ombudsman Office
- Key objective:
  - Consider information governance issues and facilitate the development of common solutions that support the interoperable EHR.

20





**Information on Infoway,  
projects underway across Canada,  
and resource materials, are available on  
the Infoway website**

**[www.infoway-inforoute.ca](http://www.infoway-inforoute.ca)**

**Contact Information**

Joan Roch, Chief Privacy Strategist

Canada Health Inforoute/Inforoute Santé du Canada  
1000, rue Sherbrooke Ouest, Suite 1200 Montreal, QC, H3A 3G4  
Toll Free: 1-866-868-0550 Fax: 514-868-1120

**Creating Healthy Connections**

## **Electronic Health Information and Privacy Survey: What Canadians Think – 2007**

**Mary Lysyk, Policy Advisor, Health Canada**


### **Abstract:**

Ms Lysyk will provide a brief report on the recently completed public opinion research into "What Canadians Think" about electronic health information and their privacy. This research was undertaken jointly by Canada Health Infoway, Health Canada and the Office of the Privacy Commissioner of Canada. It builds on work previously conducted by the three organizations separately. The findings hold interesting implications for discussions of governance in the EHR."

### **Bio:**

Lysyk 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.





Health  
Canada


Santé  
Canada


## ***Electronic Health Information and Privacy Survey What Canadians Think – 2007***

Co-sponsored by:  
Canada Health Infoway  
Health Canada  
Office of the Privacy Commissioner of Canada

Conducted by:  
Ekos Research Associates

Presentation for:  
Electronic Health Information and Privacy  
Conference, Ottawa, Ontario  
December 3, 2007






Health  
Canada

Santé  
Canada

## **Background**

- Over the past 5 years, studies have documented the importance of protecting privacy, confidentiality and security of personal health information, in both paper and emerging Electronic Health Record (EHR) environments.
- 2003, Canada Health Infoway, *Public Attitudes to Electronic Health Records and its Linkages*
- 2004, Health Canada, *Pan-Canadian Health Information Privacy and Confidentiality Framework*
- 2007, The Office of the Privacy Commissioner of Canada *Canadians and the Privacy Landscape*



2



Health  
Canada

Santé  
Canada

## Survey Objectives

### To measure:

- perceptions about personal privacy and privacy of personal health information
- awareness of privacy laws and oversight bodies
- perceptions and experiences related to electronic health information
- public's level of trust, comfort and tolerance for electronic health record systems
- secondary uses of electronic health information



3



Health  
Canada

Santé  
Canada

## Methods

- Telephone survey methodology
- 2,469 Canadians, 16 years and older
- Results were statistically weighted by age, gender, and region to ensure representation of the Canadian population
- Analysis was completed regionally (e.g., Atlantic region; 'Prairies' refers to Manitoba and Saskatchewan)
- Results are statistically accurate to within +/- 2.0 percentage points, 19 times out of 20



4



## Presentation of Key Findings

- I. Personal Health Information Privacy
- II. Electronic Health Information
- III. Experiences with Electronic Health Information
- IV. Electronic Health Information and Privacy
- V. Measures for Increasing Comfort
- VI. Secondary Uses
- VII. Conclusion
- VIII. Moving Forward



## I. Personal Health Information Privacy

- Personal Health Information is still considered one of the most sensitive areas of personal information.
- Close to two in three Canadians (64%) believe that there are few types of personal information that are more important for privacy laws to protect.





Health  
Canada

Santé  
Canada

## Perceptions of Privacy

- When asked about the protection of their personal information in general, one in two (53%) responded that their privacy is less protected than five years ago.
- In contrast, one in three (37%) feel the same about the privacy of their personal health information.



7



Health  
Canada

Santé  
Canada

## Perceptions about Safety and Security

- Almost 8 in 10 (79%) Canadians consider health information to be at least *moderately* safe and secure.
- 39% of respondents indicated that their personal health information was *very* safe and secure.



8



## Trust Levels

- A hierarchy of trust levels to keep health information safe and secure exist.
  - Highest trust in health care professionals, e.g. doctors (86%)
  - Slightly lower trust in administrative support staff, (66%)
  - Mixed trust outside the circle of care, e.g. university researchers (52%)



9



## Privacy Breaches

- 4% of Canadians report that their personal health information has been used inappropriately or without their consent
  - *'A receptionist was talking about me to a mutual friend.'*
  - *'I was sent a letter for a fundraiser for a specific disease which I had and it came from the hospital I was treated, so someone used to see the information to see if I would donate money.'*
  - *'My doctor released my health information to a lawyer without a court order'*



10



Health  
Canada

Santé  
Canada

## Awareness of Privacy Laws and Institutions

- Awareness of privacy laws or agencies is low.
- Specifically, respondents rated awareness of the Privacy Act (laws) and the Office of the Privacy Commissioner of Canada (institutions) as highest



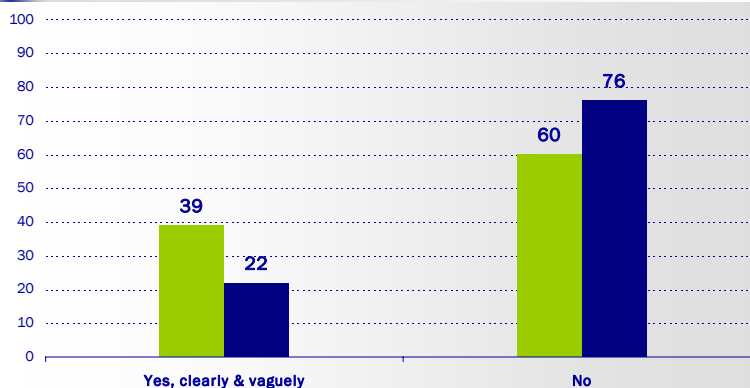
11



Health  
Canada

Santé  
Canada

## Awareness of Laws and Institutions



Q:

Are you aware of any laws / federal, provincial or territorial institutions that help Canadians deal with privacy and the protection of personal health information?

(Base: All Canadians; June/July 2007, n= half sample)



12



## II. Electronic Health Information- General Perceptions

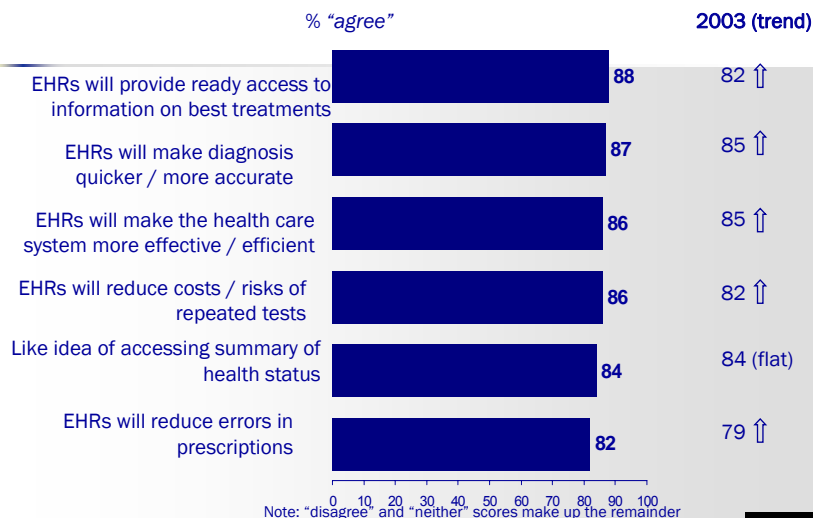
- Support for EHRs is on the rise. Close to 9 in 10 (88%) support the concept.
- Perceptions of overall advantages of the EHRs are numerous.



13



## Potential Advantages of EHRs

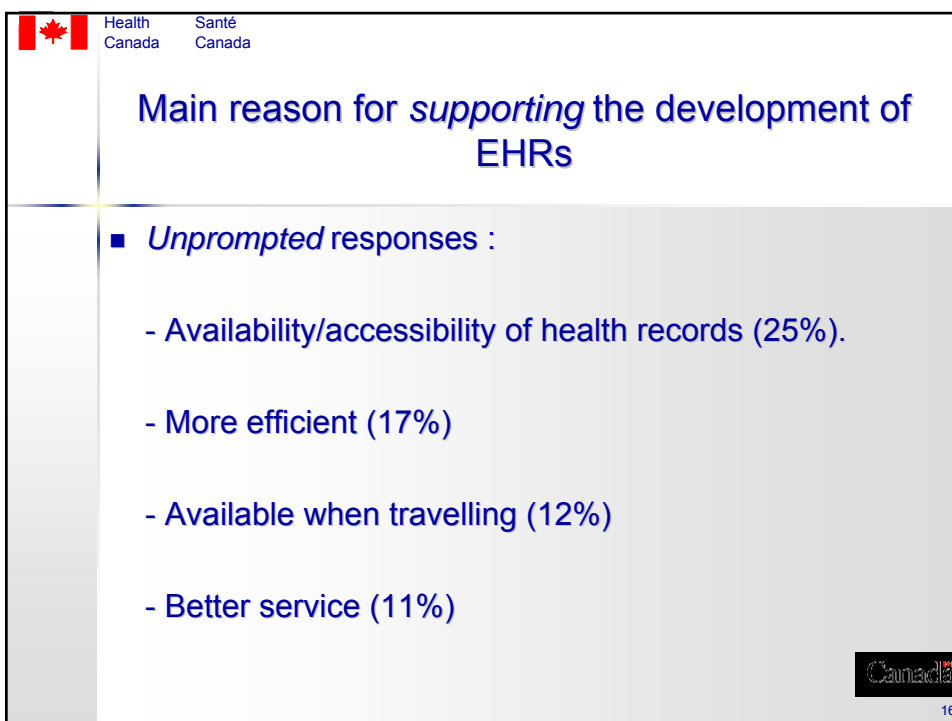
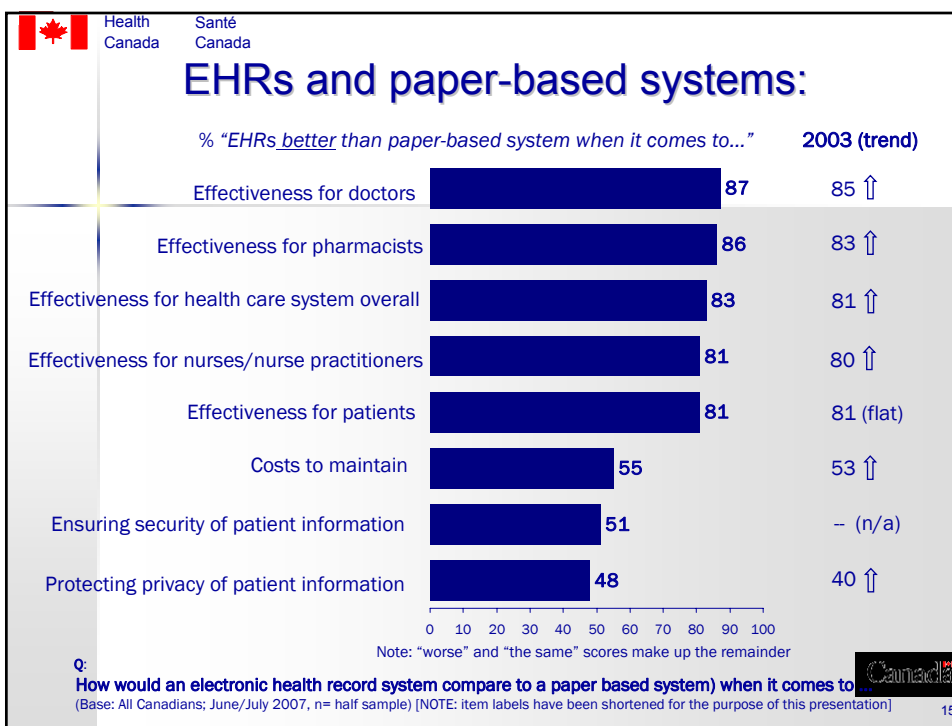


Q:

There are a number of arguments made for and against electronic health records. How much do you disagree with the following arguments? [NOTE: Item labels have been shortened for the purpose of this presentation] (Base: All Canadians; June/July 2007; n = half sample)



14







Health  
Canada

Santé  
Canada

## Electronic Health Information- Respondent Quotes

- *"We travel out of province and access to all health information in case of an emergency would be valuable"*
- *"They had everything right there..saved me from a drug interaction that may have cost me my life"*
- *"Better health care due to better access to information."*
- *"It's just a good idea"*



17



Health  
Canada

Santé  
Canada

## III. Experience with Electronic Health Information

- A new measure: One in three (31%) reported interaction with electronic health information.



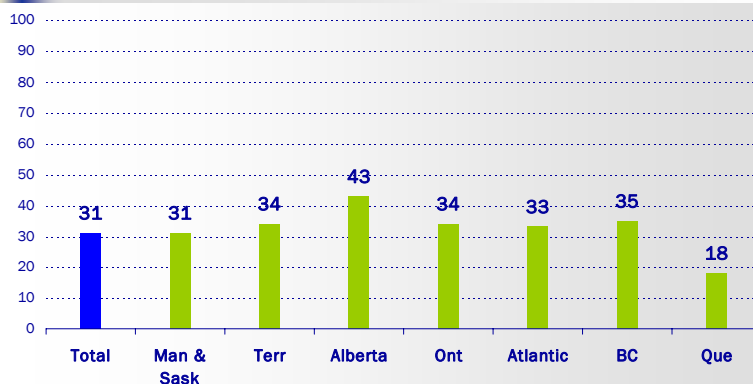
18



Health  
Canada

Santé  
Canada

## Experiences with electronic health information - by Region



Q:

In the past year, have you had any interaction with a health care provider that used some type of electronic health information system? Please do not include those interactions where someone verified your name, address and health card information using computers upon your arrival. Base: All Canadians; June/July 2007, n= half sample)



19



Health  
Canada

Santé  
Canada

## A Closer Look at Interactions....

Those reporting experience with electronic health information show interesting trends:

- Greater awareness of privacy laws (51% vs. 39%)
- Belief that EHRs would be better at protecting personal health information compared to paper systems (52% vs. 48%)
- Overall opinion that the health care system would be more effective and efficient compared to paper system (89% vs. 83%)



20



## A Closer Look at Interactions....

Unprompted impressions of electronic health information included (N=762):

- one in three (36%) describe the experience as generally positive
- health care service delivery was faster (23%)
- information was more accessible (11%)
- more neutral impression (22%)



21



## Experience with Electronic Health Information - Respondent Quotes

- *'It was communicative, It was specific and zeroed in on my history'.*
- *'I loved it because it was easy..there were computers in every exam room..they typed up your name and your whole file, everything came up.'*
- *'It was fine; makes everything faster'*
- *'I am a skeptic: Until it is centralized and access is limited, I'm not impressed'*



22



### III. Electronic Health Information and Privacy

- Canadians' specific concerns about EHRs are primarily focused on privacy and security issues and include:
  - access for malicious purposes (45%)
  - use for unwanted purposes in the future, e.g. unauthorized secondary uses (42%)
  - that privacy and security procedures would not be followed (37%)



23



### Electronic Health Information and Privacy- Respondent Quotes

- *'It is a good idea. It is easier to access information, but [I am] concerned about unauthorized usage'*
- *'The electronic systems are not foolproof. Someone could enter the system with malicious intent'*
- *'If I had things I didn't want people to know, I would be more concerned about that information getting out.'*
- *'We trust banking electronically, so we can trust electronic health records using proper encryption and proper storage.'*



24



## IV. Measures for Increasing Comfort

- Canadians have identified at least 8 measures to protect their information in electronic environments.
- Support for these measures has increased since 2003.
- All of the measures increase comfort with EHR systems.
- **Note:** Support for the measures is stronger in those who reported experience with electronic health information.



25



## Increasing Comfort with Electronic Health Information

### Canadians want:

- Audit trails (77%)
- Strong penalties for unauthorized access (74%)
- Being informed of privacy and security breaches (70%)
- The ability to access, verify and report corrections to their record (68%)
- Clear privacy policies (66%)



26



## Increasing Comfort with Electronic Health Information

### Canadians want (cont'd):

- Physicians endorsement of the system (66%)
- Breach protocols (65%)
- System oversight (61%)
- The ability to hide/mask sensitive information (55%)



27



## Secondary Uses

- Canadians express some openness to EHRs being used for health research purposes.
  - More than 8 in 10 support use in health research provided that personal details are not known to researchers.
  - If personal details are not removed, support drops to 50%.
  - 66% support health researchers linking personal health information to other records that may be related to health outcomes (e.g., income, education), if consent is obtained.



28



## Conclusions

- Awareness and support for EHRs continues to grow. Positive views strengthen with experience.
- Clearly, Canadians appreciate the potential benefits of EHRs, including overall health care effectiveness and efficiency.
- The public currently has considerable trust in health information custodians, particularly within the circle of care.
- Protecting personal health information privacy, confidentiality and security remains paramount.



29



## Moving Forward

- Current initiatives to support Canadians' privacy and security expectations:
  - Canada Health Infoway's Blueprint includes privacy and security component and numerous features to increase comfort with EHRs (e.g., audit trails)
  - *Pan Canadian Health Information Privacy and Confidentiality Framework* developed to respond to Canadians privacy and confidentiality expectations.



30



Health  
Canada

Santé  
Canada

*"If you can protect my privacy, I am okay with  
[electronic health records]..."*

  
31



Health  
Canada

Santé  
Canada

**Mary Lysyk,**  
Access to Information and Privacy Division.  
Health Canada  
[mary\\_lysyk@hc-sc.gc.ca](mailto:mary_lysyk@hc-sc.gc.ca)

  
32



## **eHealth in BC: A Work in Progress**

**John Cheung, Executive Director, eHealth Privacy, Security and Legislation, Knowledge Management and Technology Division, Ministry of Health, Government of British Columbia**

### **Bio:**

John Cheung has worked in the health care sector for close to 30 years. Within the BC Ministry of Health, John has occupied a number of senior executive and management positions. Some of his previous responsibilities include managing programs and services such as hospital programs, provincial and tertiary health services, home and community care programs, medical services plan and health services policy development. In the early 90's, prior to the formation of regional health authorities, he was appointed to develop and lead a pilot project in BC to integrate health care services in a single structure known as Comprehensive Health Organization. John has always been a strong supporter of evidence based decision-making and has been a power user of health data through out his health services management career.


Because of his interest and background in health data, he decided to retire from health program and service management and focus his effort in health information management. John was appointed about 6 years ago as the Executive Director, Information Resource Management, responsible for all of Ministry of Health databases and decision support services. In addition, he was responsible for the Ministry's privacy and freedom of information protection, record management services, information system security and library services. He was also the chief data steward for the Ministry of Health responsible for access to all Ministry's health data.

In the beginning of 2007, with eHealth well underway, John was re-assigned to his current position of Executive Director, eHealth Privacy, Security and Legislation. This position is responsible for developing all health information legislations, privacy and security protection policies necessary to guide the design and enable implementation of eHealth projects.


**Bill Trott, Director, Integration for eHealth Privacy and Legislation, BC Ministry of Health**

### **Bio:**

Bill Trott, Director, Integration for eHealth Privacy and Legislation, Ministry of Health, worked acting director and portfolio officer in the Office of the Information and Privacy Commissioner of British Columbia, Offices of the Ombudsman in British Columbia and Ontario, Psychiatric Patient Advocate Office, Province of Ontario, Ministry of Health, Province of Ontario and the Community Legal Assistance Society in Vancouver, BC. He graduated from the Faculty of Law, University of Victoria in 1981 and was adjunct professor in the Faculty of Law at UBC (1992-1995). His publications include "Freedom of Information and Protection of Privacy" in Annual Review of Law and Practice, The Continuing Legal Education Society of British Columbia (1998, 1999, 2000 and 2001); and a chapter in A Legal Handbook for the Helping Professional, Second and Third Editions, Law Foundation of British Columbia, 1998 and 2006. He has served on several boards of community organizations including the national Canadian Mental Health Association, Parkdale Legal Services Association, Parkdale Activity and Recreation Centre, and the Lower Mainland Purpose Youth Association.




BRITISH COLUMBIA



# eHealth in BC A Work in Progress

*Electronic Health Information and Privacy Conference*

OCRI - December 3, 2007  
John Cheung and Bill Trott

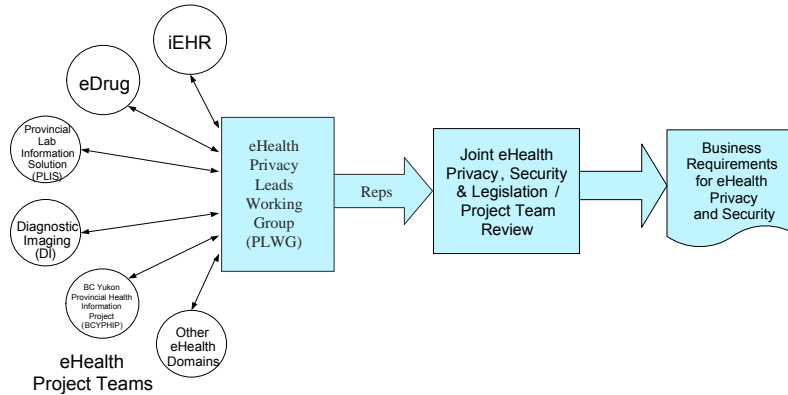


## Stakeholder Engagement and Policy Formulation Process

2



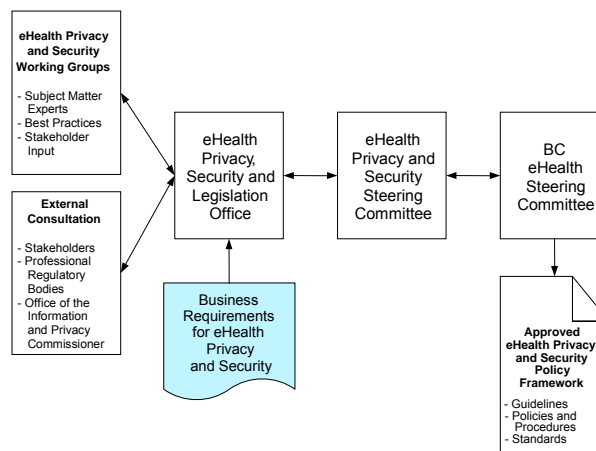
## Internal eHealth Privacy & Security Business Requirements Determination Process



3



## eHealth Privacy & Security Policy Framework Development Steps



4



## Key Components for Privacy and Information Security Governance Structure

- Legislation and Legal
- Disclosure (consent) Directive
- Identity Management
- Access Control Management
- Audit and Logging
- Privacy and Security Breach Management
- Secondary Use
- System Security
- Records Retention

5



## Current Status

### Legislation and Legal:

- Amendments made to authorize the indirect collection of data for health related purposes.
- New provisions were based on existing provisions in the *Health Act* - BC Cancer Agency and Health Status Registry.
- Amendments require data registries in the custody or control of MoH or HAs to be designated by the Minister as "health information banks" (HIBs).
- More amendments to be introduced in spring 2008 to provide legislative authority for disclosure directives and others.
- eHealth Information Sharing Agreement being drafted.

6



## Current Status – cont'd

- Foundation policy framework established for disclosure directives, identity management, access control management, audit and logging, privacy and security breach management.
- Providing policy input to iEHR and PLIS Projects for completion of business requirements.
- Initiated stakeholder consultation and review work on secondary use.
- Continuing work with stakeholders on policy details.

7



## Health Data – current and future

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>■ Current               <ul style="list-style-type: none"> <li>– MSP billing (includes diagnosis)</li> <li>– Discharge abstract data</li> <li>– Home and community care</li> <li>– Mental Health (not clinical chart)</li> <li>– Addiction data</li> <li>– PharmaCare claims</li> <li>– PharmaNet (medication history) – no direct access</li> <li>– Vital Statistics</li> <li>– Client Registry</li> <li>– Provider Registry</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>■ Future               <ul style="list-style-type: none"> <li>– Lab clinical results</li> <li>– Diagnostic Imaging</li> <li>– Additional drug data</li> <li>– Core data set from physicians in private practice</li> </ul> </li> </ul> |
|---|---|

8



# Roles Based Access Controls

9



## Provincial eHealth Access Management Control Policy is based on...

1. User Identity Management Strategy 
2. "Chain of accountability" that attributes direct responsibility for each user to a regulated health care professional or approved organization
3. Limits on ability to grant access (central authority or approved organization) 
4. Roles and Permissions - a strict "need to know" for specific job function
5. Educating users about their privacy and security responsibilities and accountabilities
6. Attestation upon user access to an individual's information that access is for the purpose of clinical care
7. Individual Disclosure Directives 
8. Limitations on search functionality to impede browsing  

10



## Provincial eHealth Access Management Control Policy is based on...

9. Use of pro-active and re-active audit mechanisms
10. Setting and publicizing significant penalties for unauthorized access, up to and including termination of employment
11. Restrictions on storage of, and access to personal information outside Canada (as required by *FOIPPA and Health Act*)
12. Working with regulatory bodies to provide them with information and reports to facilitate monitoring of their members' compliance with conditions of access
13. Mechanisms to remind users of their privacy obligations
14. Functional capacity for central revocation of access
15. Additional technological and administrative privacy-enhancing features that meet industry standards and best practices.

11



## Granting access to EHR information

- Only a central authority or an "approved organization" will be permitted to grant access to EHR information. An "approved organization" must



- comply with minimum privacy and security policy requirements (ex. Breach policy, audit policy, supply, to a central authority, a list of staff persons who are allowed to authorize access to EHR information)
- enter into an Information Sharing Agreement (ISA) that lays out terms and conditions for approval and ongoing approved status

12



## Supervising Provider and Supervised User

- In an organization that is not "approved", each user must be either a
  - Regulated health professional
  - or
  - Supervised user acting on behalf of, under the responsibility of, and under the direct supervision of a regulated health care professional
- When supervised persons access information on behalf of their supervising providers their relationship must be specified
- Supervised users must have own unique User ID
- Access approval must still be given by a third party
- [Supervising Provider access revocation](#) ➡ [Supervised User access revocation](#)
- Regulated health care professionals are not permitted to supervise the access of other regulated health care professionals
- Conditions of becoming a supervised user or supervising provider will be part of an access agreement

13



## Roles and Associated Permissions

- Single set of EHR roles
- Approved organization must assign user roles appropriately
- Roles and permissions must reflect job needs
  - Standardized EHR modules that can be appended to existing roles might be able to reflect this reality
- EHR roles must be provincially managed, and cannot be modified locally
- All EHR user roles should have a set of core transactions to enable them to accurately identify the individual whose information is to be accessed
- Clinical versus administrative roles



14





## Assignment of Role and Approval of Access

1. Must be a role request, providing required information
2. Role assignment and access approval must be carried out by different persons
  - List of persons with authority to approve access must be maintained centrally
3. Conditions of access
  - Privacy Education and User Training
  - User agreement (confidentiality, compliance with security requirements, etc.)
4. Access renewal
  - Annual
  - Process leveraged to refresh user on privacy and security requirements
5. Change management process to manage evolving roles
6. Role de-commissioning
7. Appeal mechanism available if access denied

15



## Privacy and Security Meet Design

16



## Privacy and Security Policy meet Design

- iEHR team "translates" policies into business requirement documents (BRDs)
- Matrix template designed for iEHR team to map how the policies are met in requirements
- All policy statements assessed - business requirement or assigned to another phase
- Mapping of each policy statement to assumptions, use cases, and requirements found in 20 BRDs
- SUN will provide Province with design requirement documents based upon business requirements
- iEHR team to map design to policies

17



## Governance

18



## Governance - Central functions

- Set-up:
  - Provincial role definitions;
  - Approved organization criteria and granting of status;
  - Templates for ISA, confidentiality agreements, and user agreement;
  - Connectivity compliance and technical message testing;
  - Determination of custody/control of data.

19



## Governance - Central functions

- On-going operations, management and administration:
  - Breach policy investigations and incident management;
  - Role assignment in non-approved organizations;
  - Disclosure directive administration;
  - End-to-end auditing – e.g. audit of privileged users - system administrators;
  - Disaster recovery;
  - Training materials;
  - Secondary use access oversight.

20



## Governance - Central functions

- Provincial common strategy:
  - Identity proofing policy and process;
  - Authentication and Certificate Authority

21



## Lessons Learned

22



## Lessons learned

- Stakeholder engagement process is critical – must be transparent;
- Identify the correct stakeholders – providers and public;
- Detailed mapping of business requirements to privacy and security policy key to accountability;
- Define the planning cycle well in advance – how to plug privacy and security into the project plan;
- This is hard work – better to do it up front – this is a continual process.

23

## **Panel 3A: Emerging Healthcare Technologies and the Future of Privacy**

**Chair: Ian Kerr, University of Ottawa**

### **Panel Overview:**

This panel investigates future challenges to the preservation of privacy arising from the adoption of new and emerging health technologies. Moving from the present to the near future and beyond, panelists will examine genetics, assisted reproductive technologies and nanotechnology to interrogate the future of privacy.

### **Biography of Chair:**

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.

Ian 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.

## **Negligence Liability for Breaches of Data Security**

**Jen Chandler, University of Ottawa**

### **Abstract:**

Breaches of data security have become extremely high-profile news. Numerous lawsuits have been filed in North America particularly in relation to breaches in the security of financial data and the problem of identity theft. However, there have also been negligence claims relating to the careless disclosure of medical data. With the creation in Ontario of a statutory duty to notify those affected by breaches in the security of their health information, it is possible that litigation will increase. As emerging medical technologies permit the collection of new types of information that identify predisposition to illness (e.g. genetic data) or that directly affect other parties (e.g. medical data relating to assisted reproductive technologies and genetics), the nature of the harms flowing from the disclosure of medical information as well as the identity of potential plaintiffs may change.

### **Bio:**

Jennifer A. Chandler is an assistant professor at the Faculty of Law, University of Ottawa. She has a BSc in Biology (University of Western Ontario), as well as an LLB (Queen's University) and LLM (Harvard University). She currently teaches undergraduate courses in tort law and medical law and a graduate course in law and technology theory. Her main research interest is in the area of law, science, and technology.

# Negligence Liability for Breaches of Data Security

Electronic Health Information and Privacy Conference,  
December 3, 2007, Ottawa

Professor Jennifer A. Chandler  
Law & Technology Program, Faculty of Law

Law & Technology Program  
University of Ottawa

Université d'  
University of  
**Ottawa**  
L'Université canadienne  
Canada's university

The screenshot shows the CBC News website interface. At the top, there's a navigation bar with 'cbc.ca' and links for News, Sports, Entertainment, Radio, TV, and My Region. Below this is a red banner for 'CBCnews CANADA | NFLD. & LABRADOR'. The main headline reads 'N.L. police probe security breach of patient information'. To the left is a sidebar with a list of Canadian provinces and territories, with 'Newfoundland & Labrador' highlighted. The main content area contains a paragraph about the breach, stating that officials are investigating a computer security breach involving sensitive patient information. To the right of the main text are two sidebars: 'MORE NFLD. & LABRADOR HEADLINES' with links to oil spill, Harper's status, and Placentia Bay refinery; and 'CANADA FEATURES' with links to 'Interactive Smarty pants' and 'Arts Crazy for Alice'.

cbc.ca News Sports Entertainment Radio TV My Region Search CBC.ca

**CBCnews** CANADA | NFLD. & LABRADOR

Story Tools: E-MAIL | PRINT | Text Size: S M L XL | REPORT TYPO | SEND YOUR FEEDBACK

## N.L. police probe security breach of patient information

Last Updated: Saturday, November 24, 2007 | 12:29 PM NT  
[CBC News](#)

Officials in Newfoundland and Labrador are investigating a computer security breach involving sensitive patient information that may have been accessed through the internet.

The data, including lab test results for infectious diseases such as HIV and hepatitis along with patient names and health numbers, was stored on a government desktop computer, said Health Minister Ross Wiseman.

The computer was unplugged and taken to the home of a consultant working for the Provincial Public Health Laboratory, something Wiseman said should never have happened.

"That was an inappropriate use. Obviously individual computers that are available for work are there for the workplace only," he told CBC News.

On Friday, Attorney General Jerome Kennedy called the security lapse a "very serious matter that required immediate action" to determine whether there has been "any illegal activity or hacking."

On Tuesday night, someone claiming to be a computer security specialist from somewhere outside the province called the consultant

**MORE NFLD. & LABRADOR HEADLINES »**

- Oil spill closes section of industrial park
- Harper to announce status for some Mi'kmaq
- Second Placentia Bay refinery closer to reality
- Williams to meet Harper on Friday
- Respect prisoners' privacy: citizens' representative

**CANADA FEATURES**

**INTERACTIVE**  
**Smarty pants**  
Are you smarter than a Russian 4<sup>th</sup> grader?

**ARTS**  
**Crazy for Alice**  
Why is Alice Munro so big with European shrinks?

Source: [www.cbc.ca](http://www.cbc.ca)



BBC News 24

News services  
Your news when you want it

News Front Page  
World  
UK  
England  
Northern Ireland  
Scotland  
Wales  
Business  
Politics  
Health  
Education  
Science/Nature  
Technology  
Entertainment  
Also in the news  
Video and Audio  
Have Your Say  
Magazine  
In Pictures  
Country Profiles  
Special Reports  
RELATED BBC SITES  
SPORT  
WEATHER

Last Updated: Tuesday, 20 November 2007, 19:51 GMT  
E-mail this to a friend  
Printable version

## UK's families put on fraud alert

**Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing.**

The Child Benefit data on them includes name, address, date of birth, National Insurance number and, where relevant, bank details of 25 million people.

Chancellor Alistair Darling said there was no evidence the data had gone to criminals - but urged people to monitor bank accounts "for unusual activity".

The Conservatives described the incident as a "catastrophic" failure.

In an emergency statement to MPs, Mr Darling apologised for what he described as an

The chancellor urged people to monitor their bank accounts

**WATCH** Alistair Darling

### BENEFIT RECORDS LOST

**KEY STORIES**

- Data disc report 'in three weeks'
- Discs 'worth £1.5bn' to criminals
- Data minister 'not told of discs'
- Six more data discs 'are missing'
- Private data 'also given to firm'
- Cameron calls for ID cards halt
- Threat of fraud 'looms for years'
- Brown apologises for records loss
- UK's families put on fraud alert

**Queries answered**  
BBC personal finance reporter Jennifer Clarke answers your questions on the crisis

**FEATURES AND BACKGROUND**

- Q&A: Child benefit records lost
- Government letter: full text
- Taking cover from ID theft
- Point-by-point: Darling statement
- The dealers in data
- Life inside the beleaguered HMRC
- Timeline: Benefits records loss

### CHILD BENEFIT HELPLINE

+ 0845 302 1444

Source: [www.bbc.co.uk](http://www.bbc.co.uk)

		as an auditor. Veterans Affairs' officials have said only 185,000 numbers are at risk because many were repeated in the file.	
Nov. 17, 2007	Ohio Masonic Home / Battelle & Battelle LLC (Springfield, OH)	A laptop stolen from a Kettering auditing firm contained personal information on employees of up to 10 businesses, including Springfield-based Ohio Masonic Home. Battelle & Battelle LLC would not disclose the number of individuals affected by the theft but Masonic Home officials said 600 of its employees' information was stored in the laptop.	600
Nov. 21, 2007	University of Florida (Gainesville, FL) Those who suspect their Social Security numbers were posted can search their names on the Web site <a href="http://www.ssnbreach.org">www.ssnbreach.org</a>	More than 400 former UF students might have been put at risk for identity theft after their Social Security numbers were posted on UF's Computing & Networking Services Web site. A news release from the Liberty Coalition, a group that works to preserve the privacy of individuals, said 14 files on the Web site contained "sensitive information" of 534 former UF students, including 415 Social Security numbers.	415
Nov. 21, 2007	United Healthcare (New York, NY)	United Healthcare posted the Social Security numbers of doctors at Columbia University's faculty practice on a public Web site. United posted the taxpayer identification numbers, some of which were Social Security numbers, alongside the names of 993 providers at Columbia who participate in the insurer's network. The list was supposed to be accessible to Columbia employees during the current open enrollment period.	Unknown
TOTAL number of records containing sensitive personal information involved in security breaches			216,176,736

Source: [www.privacyrights.org](http://www.privacyrights.org) "A Chronology of Data Breaches"

## Civil lawsuits (so far...)

### •Canada

- *Speevak v. Canadian Imperial Bank of Commerce* (filed Ont. S.C.J. 2005)
- *Taylor et al. v. Queen in Right of Saskatchewan (Worker's Compensation Board) et al.* (filed 2003, Sask. Q.B.)
- TJX Companies lawsuits (filed 2007)
- Talvest lawsuits (filed 2007)



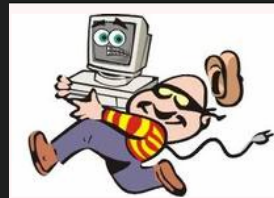
## Civil lawsuits (so far...)

### •United States

• *Randolph et al v. ING Life Insurance and Annuity Co.* (2007 D.C.); *Bell v. Acxiom Corp.* (2006 E.D. Arkansas); *Richardson v. DSW, Inc.* (2005, 2006, N.D. Ill.); *Giordano v. Wachovia Securities LLC et al* (2006 Dist. N.J.); *Stollenwerk et al v. Tri-West Healthcare Alliance* (2005 Dist. Ariz.); *Tracy L. Key v. DSW, Inc.* (2006 S.D. Ohio); *Hendricks v. DSW Shoe Warehouse Inc.* (2006 W.D. Mich.); *Kuhn v. Capital One Financial Corp. Inc.* (2004 Supt. Ct. Mass); *Guin v. Brazos Higher Education Service Corp. Inc.* (2006 Dist. Minn.); *Forbes v. Wells Fargo Bank* (Dist. Minn, 2006); *Jones v. Commerce Bancorp, Inc. et al* (2006, S.D. N.Y.); *Bell v. Michigan Council 25*, (2005 Mich. C.A.); *Daly v. Metropolitan Life Insurance Co.*, (2004 N.Y. Sup. Ct.); *Huggins v. Citibank N>A. et al.* (2003, Cal.); *BJ's Wholesale Club litigation* (2005, 2006).

### •Major Ongoing Class Actions

- Cardsystems lawsuits
- Choicepoint lawsuits
- TJX lawsuits.



# What types of security breaches?

- Hacking into poorly secured networks and databases
- Misdirected faxes
- Careless disposal of records
- Website security flaws
- Loss or theft of records (in hardcopy or electronic form)
- Employee theft of information
- Loss or theft of records from third party service providers.


A photograph of a man with a beard and sunglasses, wearing a purple patterned vest over a black shirt and blue jeans, sitting in a black office chair at a desk. He is looking at a laptop screen. On the desk, there is a CRT monitor, a keyboard, and various other items. A white trash can is on the floor next to the desk. The background is a plain wall.

- 



# Transition to Electronic Health Records

- Ease of storage, transmission, retrieval.
- Ease of inadvertent disclosure, transmission.
- Attractive target for theft, misuse.

A photograph of a row of yellow file folders in a filing cabinet. Each folder has a colorful tab with a name on it. The names visible include JON, JOR, JUA, K, KEE, and KEL. The tabs are in various colors like red, green, blue, and yellow. The folders are arranged in a row, and the image is slightly out of focus, emphasizing the transition from physical records to electronic ones.

- 



## Health information and negligence

- *Peters-Brown v. Regina District Health Board* (1995 Sask Q.B., affirmed 1996 Sask. C.A.)



- *Mammone v. Bakan* (1989, B.C.S.C.)

## Types of Harms

- What type of data?
  - health card information
  - identity information (name, address, date of birth)
  - health status (condition, treatment, prognosis)
  - financial data (payment cards, private insurance details)
- What type of use of the data?
  - health card fraud
  - employment decisions
  - private insurance
  - financial fraud
  - social consequences, humiliation

## Negligence and Data Security Breaches

### Legal issues

- (1) Duty of Care: Is the data custodian responsible for the intervening criminal acts of a third party?
- (2) Has the plaintiff suffered “actual harm” before misuse of the information occurs?
- (3) Can the plaintiff demonstrate causation after misuse of the information occurs?



### (1) Duty of Care

- Is there a duty of care owed to patients to protect the confidentiality of medical information?
  - Well-established duty of care at common law owed by health care providers to their patients and customers.
  - Statutory duties in relation to data – e.g. s.12(1) *PHIPA*
    - “a health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure ...”
- Do these duties extend to protecting against the criminal wrongdoing of third parties?
  - *M. H. v. Bederman* (1995, Ont. G.D., new trial ordered 1997, Ont. Div. Ct.)



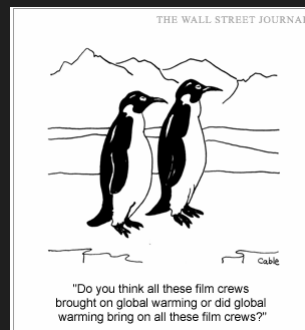
## (2) Actual Harm

- What kind of harm is at issue?
  - physical harm (to property or person)
  - mental distress
  - economic losses
- Is there any harm before a third party misuses the confidential information?
  - "Plaintiff's claims are based on nothing more than speculation that she will be a victim of wrongdoing at some unidentified point in the indefinite future." *Key v. DSW Inc.* (S.D. Ohio, 2006).



## (3) Causation

- Was the data that was misused obtained from the defendant?
  - Sometimes difficult to prove this in the context of financial data, which is commonly shared with others (e.g. credit card numbers).
  - but not impossible... *Bell v. Michigan Council 25* (Mich. C.A. 2005).
  - Probably not as difficult to prove in the medical context.



## What is reasonable care?

- Sources of information
  - Decided cases
  - Statutory data safeguard obligations (*PIPEDA*, provincial privacy protection legislation).
  - Decisions of the federal and provincial Privacy Commissioners.



## Clues in the ID Fraud Case Law (page 1)

- Plaintiffs' claimed breaches of the standard of care
  - Failure to protect physical premises against theft of data.
  - Failure to protect physical property such as laptops on which data resides.
  - Carelessness in permitting employees to take unencrypted sensitive information home, where it is subsequently stolen or misused by third parties.
  - Failure to use proper computer network security measures.
  - Unauthorized retention of information.
  - Failure to follow Payment Card Industry security standards and rules.



## Clues in the ID fraud Case Law (page 2)

- Plaintiffs' claimed breaches of the standard of care
  - Carelessness in selecting and supervising third party contractors.
  - Carelessness in using the fax machine
  - Failure to train and supervise employees regarding privacy.
  - Failure to use encryption and secure communication lines.
  - Failure to implement proper governance procedures to ensure management is aware of security and privacy problems.
  - Failure to inform affected individuals promptly of a breach in data security.



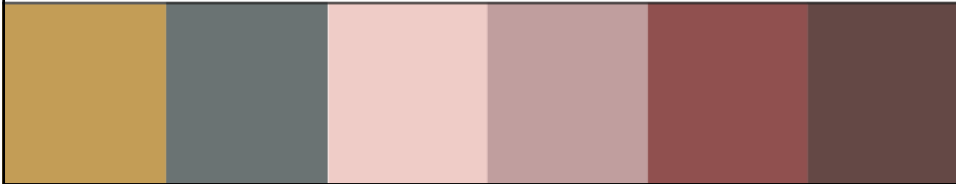
## Conclusion

- Plaintiffs are actively pursuing retailers and financial institutions for data security breaches leading to identity theft.
- Liability in negligence may ensue from carelessness in protecting electronic health information.
- As medical technology advances, the nature of the harms that might result from the compromise of health information may shift.
  - genetic data – consequences for family members
  - data on assisted reproductive technologies – consequences for family relationships





Professor Jennifer A. Chandler  
[chandler@uottawa.ca](mailto:chandler@uottawa.ca)



# The Privacy Implications of Assisted Human Reproduction

Vanessa Gruben, University of Ottawa

## Abstract:

Traditionally, infertility and the use of assisted reproductive technologies were intensely private, often secret, matters. Nevertheless, significant health information is gathered in the context of assisted human reproduction. Health information relating to the donor, the user, the gametes, the in vitro embryos and the procedures used must be collected, and in certain circumstances, disclosed. Much of this health information is genetic and thus has potentially wide-ranging privacy implications for both the individual and those genetically related to him/her. The collection and disclosure of this information is governed by several statutes including the *Assisted Human Reproduction Act*, *Privacy Act*, *Access to Information Act*, *Personal Information Protection and Electronic Documents Act*. This presentation will describe the complex statutory scheme governing reproductive health information. It will also explore some of the difficult issues that arise in the context of assisted human reproduction including whether the donor should be subject to an ongoing duty to disclose health information to his/her offspring and the potential is use/use of this genetic information in other contexts.

## Bio:

Vanessa T. Gruben is an assistant professor at the Faculty of Law, University of Ottawa. She has a BScH in Life Sciences from the Queen's University, an LLB from the University of Ottawa and an LLM from Columbia University. Her principal areas of interest are health law and assisted human reproduction.

# Privacy & Assisted Human Reproduction

Electronic Health Information & Privacy Conference  
December 3, 2007, Ottawa

**Professor Vanessa Gruben**  
University of Ottawa, Faculty of Law

## *Assisted Human Reproduction Act*

s. 3(1) “health reporting information”:

- (a) the identity, personal characteristics, genetic information and medical history of donors of human reproductive material and *in vitro* embryos, persons who have undergone assisted reproduction procedures and persons who were conceived by means of those procedures....

## *Assisted Human Reproduction Act*

- (1) Persons who have undergone assisted reproduction procedures
  - maintain use of technology private
- (2) Donors of reproductive materials & *in vitro* embryos
  - donor anonymity
  - *Cheskes v. Ontario (A.G.)*, [2007] O.J. No. 3515
  - may impact obligations under family law

## *Assisted Human Reproduction Act*

- privacy provisions:
  - Licensee, ss. 14-16
    - controlled activities
  - Agency, ss. 17-19
    - established by s. 21

## *Assisted Human Reproduction Act*

- part of complex web of federal and provincial privacy statutes including:
  - *PIPEDA* (or substantially similar statutes)
  - *Privacy Act*
  - *Access to Information Act*
  - other provincial privacy statutes

## *Assisted Human Reproduction Act*

- consent
- s. 14 (1) A licensee shall not accept the donation of human reproductive material or an *in vitro* embryo from any person for the purpose of a controlled activity, and shall not perform a controlled activity on any person, unless the licensee has obtained from that person the health reporting information required to be collected under the regulations.

## *Assisted Human Reproduction Act*

- disclosure by licensee to Agency:
  - s. 15 (2) A licensee shall disclose health reporting information
  - (a) to the Agency, to the extent required by the regulations;

## *Assisted Human Reproduction Act*

Person → Licensee → Agency

## *Assisted Human Reproduction Act*

- Role of licensee:
  - carry out controlled activities
- Role of Agency:
  - creation of personal health information registry
  - Agency may use “health reporting information” for...
    - purposes of the administration of this Act; or
    - the identification of:
      - health and safety risks;
      - potential and actual abuses of human rights or ethical issues associated with assisted human reproduction;
      - other matters to which this Act applies.

## **Is There Plenty of Room for Privacy at the Bottom? nanomedicine and the future of privacy**

**Ian Kerr, Canada Research Chair in Ethics, Law & Technology, Faculty of Law, University of Ottawa**

### **Abstract:**

What would happen if modern science were capable of healing the body at the molecular level, one atom at a time? What if medical advances allowed physicians to program cells in the body to respond to fine grained control, a kind of human supercomputing on a very small scale that could detect trace particles in an organ system or provide a rapid analysis of genomes, and somehow communicate such information to a remote healthcare provider or an automated system regulating a person's body? This presentation will consider some of the key privacy implications of nanomedicine as well as the gaps in our current regulatory framework for addressing them.



# plenty of eyes at the bottom?

nanomedicine and the future of privacy



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

idtrail.org

ON THE IDENTITY  
CRISIS



richard feynman

"The principles of physics, as far as I can see, do not speak against the possibility of maneuvering things atom by atom. [I]t would be, in principle, possible ... for a physicist to synthesize any chemical substance that a chemist writes down. How? Put the atoms down where the chemist says, and so you make the substance. The problems of chemistry and biology can be greatly helped if our ability to see what we are doing, and to do things on the atomic level, is ultimately developed – a development which I think cannot be avoided."

idtrail.org

ON THE IDENTITY  
CRISIS



nanotechnology<sub>1</sub> // nanotechnology<sub>2</sub>

idtrail.org

ON THE IDENTITY  
OF  
ID10



n<sub>1</sub>

idtrail.org

ON THE IDENTITY  
OF  
ID10





invisible

idtrail.org

ON THE IDENTITY  
CRISIS



=

idtrail.org

ON THE IDENTITY  
CRISIS



surreptitious

idtrail.org

ON THE IDENTITY  
CRISIS



$n_2$

idtrail.org

ON THE IDENTITY  
CRISIS



# nanotechnology

(molecular manufacturing)



- a technology for making things by placing atoms precisely where they are supposed to go
- borrowing from nature, nanotechnology employs a bottom-up rather than a top-down manufacturing process
- programming matter
- self-replication

idtrail.org

ON THE IDENTITY OF



# drexler (engines of creation)



"Nature shows that molecules can serve as machines because living things work by means of such machinery. Enzymes are molecules that make, break, and rearrange the bonds holding other molecules together. Muscles are driven by molecular machines that haul fibres past one another. DNA serves as a data-storage system, transmitting digital instructions to molecular machines, the ribosomes, that manufacture protein molecules. And these protein molecules, in turn, make up most of the molecular machinery just described."

idtrail.org

ON THE IDENTITY OF



true believer

idtrail.org

ON THE IDENTITY  
CRISIS



program matter

idtrail.org

ON THE IDENTITY  
CRISIS





idtrail.org

ON THE IDENTITY  
TRAIL



idtrail.org

ON THE IDENTITY  
TRAIL





bottom-up // top-down

idtrail.org

ON THE IDENTIFICATION OF  
IRIS



nanomedicine

idtrail.org

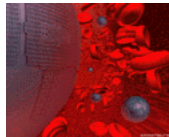
ON THE IDENTIFICATION OF  
IRIS





idtrail.org

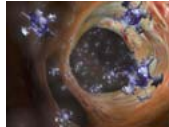
ON THE IDENTIFICATION OF  
IRIS



idtrail.org

ON THE IDENTIFICATION OF  
IRIS





idtrail.org

ON THE IDENTITY  
OF ID



idtrail.org

ON THE IDENTITY  
OF ID





idtrail.org

ON THE IDENTITY  
OF



idtrail.org

ON THE IDENTITY  
OF





idtrail.org

ON THE IDENTITY  
TRAIL



## nanomedicine

“the comprehensive monitoring, control, construction, repair, defense, and improvement of all **human biological systems**, working from the molecular level, using engineered nanodevices and nanostructures”

**glossary**, 'nanotechnology now'

idtrail.org

ON THE IDENTITY  
TRAIL



## nanosecurity

“the comprehensive monitoring, control, construction, repair, defense, and improvement of all **homeland security systems**, working from the molecular level, using engineered nanodevices and nanostructures”

[glossary](#), 'nanotechnology now'

idtrail.org

ON THE IDENTITY  
TRAIL



## nanomedicine

“the comprehensive monitoring, control, construction, repair, defense, and improvement of all **human biological systems**, working from the molecular level, using engineered nanodevices and nanostructures”

[glossary](#), 'nanotechnology now'

idtrail.org

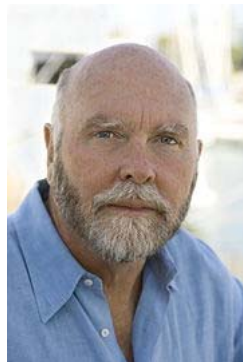
ON THE IDENTITY  
TRAIL



nanomed as surveillance

idtrail.org

ON THE IDENTITY  
CRISIS

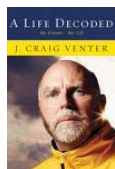


j craig venter

idtrail.org

ON THE IDENTITY  
CRISIS





idtrail.org

ON THE IDENTITY  
CRISIS

## ARCHON GENOMICS X PRIZE

[Login / Register](#)

[Archon X PRIZE for Genomics](#) [Teams](#) [News & Events](#) [Take Action](#) [Discover](#) [About](#)

Revolution Through Competition.

[TAKE ACTION](#)

### ARCHON X PRIZE FOR GENOMICS

- [Introduction](#)
- [Why Genomics?](#)
- [PRIZE Overview](#)
- [Why Whole Genome Sequencing?](#)
- [The Promise of Personalized Medicine](#)
- [Frequently Asked Questions](#)

#### PRIZE Overview

**A \$10 MILLION PRIZE  
FOR THE FIRST TEAM TO SUCCESSFULLY SEQUENCE  
100 HUMAN GENOMES IN 18 DAYS**

#### What Inspired this X PRIZE?

In 2000, Dr. J. Craig Venter led the first private team to successfully sequence a complete human genome. In the preceding decades combined governmental and private funding efforts spent \$100s of millions to develop the instrumentation required. It took the Venter team \$100 million and nine months to achieve their historic accomplishment.

The J. Craig Venter Science Foundation offered the \$500,000 Innovation in Genomics Science and Technology Prize in September 2003 aimed at stimulating development of less expensive and faster sequencing technology. To attract even more resources to this exceptionally worthy goal, Dr. Venter joined forces with the X PRIZE Foundation, wrapping his competition and prize purse into the Archon X PRIZE for Genomics.

We now invite anyone, anywhere, from any discipline to accept this grand challenge and work towards a revolutionary breakthrough in human genome sequencing.

#### The Competition Guidelines

The purpose of this X PRIZE competition is to develop radically new technology that will dramatically reduce the time and cost of sequencing genomes, and accelerate a new era of predictive and personalized medicine. The X PRIZE Foundation aims to enable the development of low-cost diagnostic sequencing of human genomes.

The preliminary guidelines for the competition have been written with this intent and will be further developed and interpreted by the X PRIZE Foundation towards this end.

The \$10 million X PRIZE for Genomics prize purse will be awarded to the first Team that can build a device and use it to sequence 100 human genomes within 10 days or less, with an accuracy of no more than one error in every 100,000 bases sequenced, with sequences accurately covering at least 88% of the genome, and at a sequencing cost of no more than \$10,000 per genome.

If more than one Team attempts the competition at the same time, and more than one Team fulfills all the criteria, then Teams will be ranked according to the time of completion. No more than three teams will be ranked and will share the prize in the following manner: \$7.5 million to the winner and \$2.5 million to the second place team if two teams are successful, or \$7 million, \$2 million and \$1 million if three teams are successful.

Actual competition events will take place twice a year with all eligible teams given the opportunity to make an attempt, starting at precisely the same time as the other teams.

For more information please see the [Competition Guidelines](#).

idtrail.org

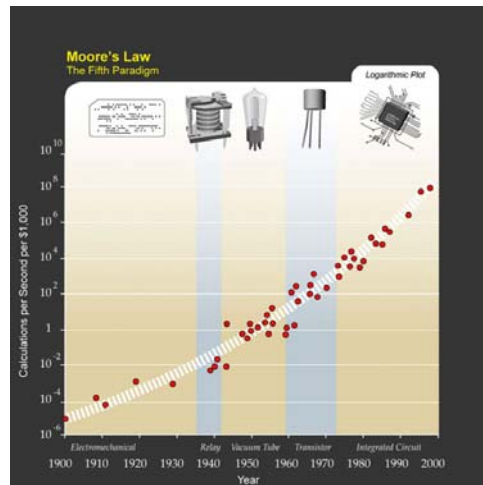
ON THE IDENTITY  
CRISIS



\$1000 genome

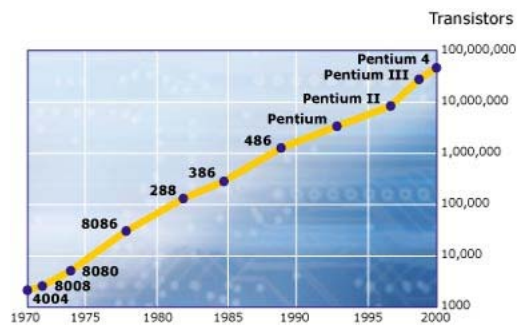
idtrail.org

ON THE IDENTITY  
CRISIS



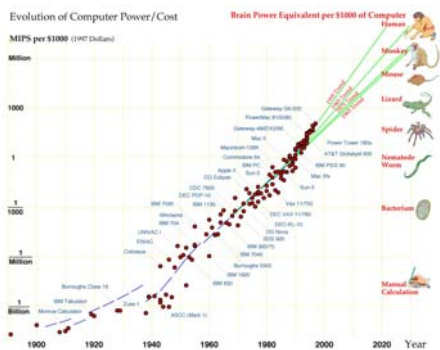
idtrail.org

ON THE IDENTITY  
CRISIS



idtrail.org

ON THE VERGE OF  
CRISIS



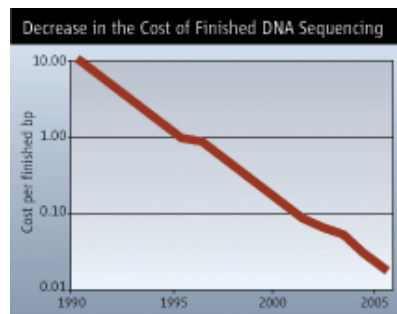
idtrail.org

ON THE VERGE OF  
CRISIS



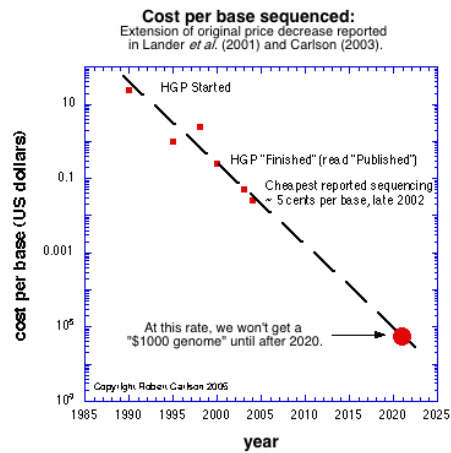
idtrail.org

ON THE VERGE OF  
CRISIS



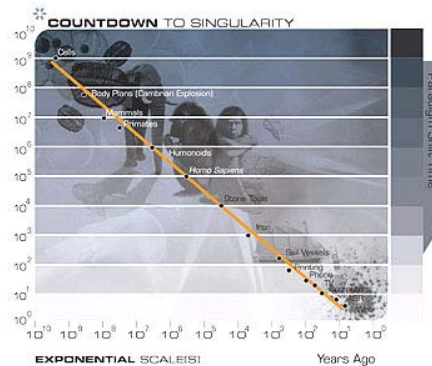
idtrail.org

ON THE VERGE OF  
CRISIS



idtrail.org

ON THE VERGE OF  
CRISIS



idtrail.org

ON THE VERGE OF  
CRISIS

dna-sms

idtrail.org

ON THE IDENTITY  
CRISIS



=

idtrail.org

ON THE IDENTITY  
CRISIS



## single molecule sequencing

idtrail.org

ON THE IDENTIFICATION OF  
IRIS



## personalized medicine

idtrail.org

ON THE IDENTIFICATION OF  
IRIS





idtrail.org

ON THE IDENTITY  
OF ID



diagnosis // cure

idtrail.org

ON THE IDENTITY  
OF ID



the “privacy” singularity

idtrail.org

ON THE IDENTITY  
CRISIS



unique molecular identifiers

idtrail.org

ON THE IDENTITY  
CRISIS





unique molecular profiles

idtrail.org

ON THE IDENTITY  
CRISIS

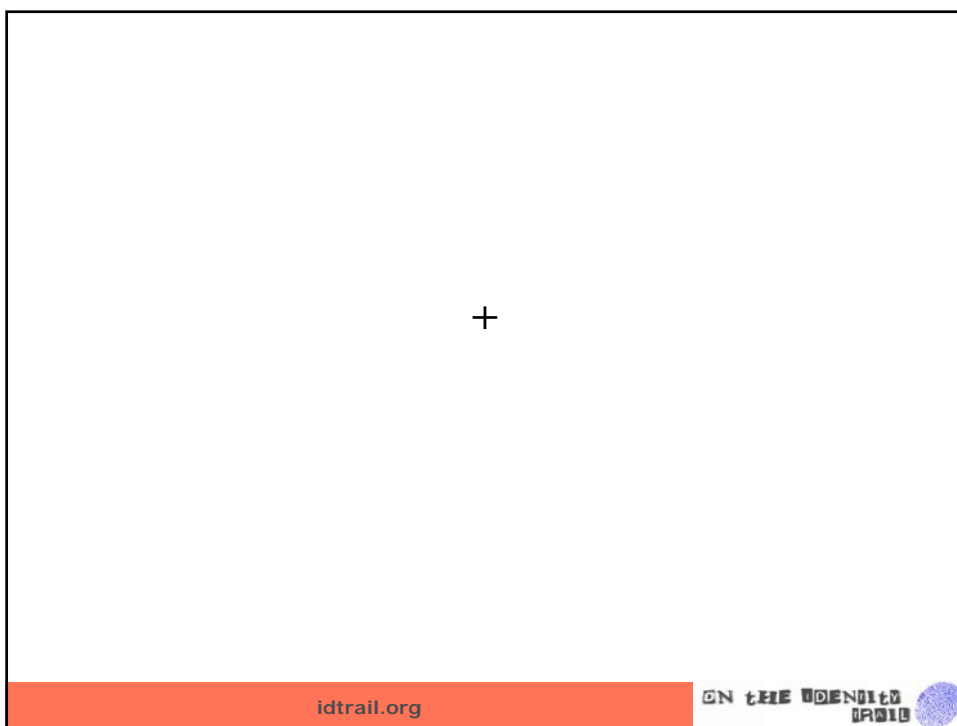


people

idtrail.org

ON THE IDENTITY  
CRISIS





2 privacy Qs?

idtrail.org

ON THE IDENTITY  
CRISIS



1.

idtrail.org

ON THE IDENTITY  
CRISIS



once readable by a \$1000 device,  
how can these identifiers be encrypted?

idtrail.org

ON THE IDENTITY  
CRISIS



huh?

idtrail.org

ON THE IDENTITY  
CRISIS



2.

idtrail.org

ON THE IDENTITY  
IPDIO



ip?

idtrail.org

ON THE IDENTITY  
IPDIO



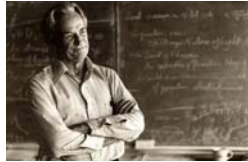
"What if you sequence my genome and find out that I have some genes with interesting and unique properties?" I asked. "Who will own that data?"

Looking at the floor with a half-smile, Venter evasively replied, "Well, you'd get a copy of the data." Did he mean I'd be licensing the data from him, the way I license Windows XP? I asked for clarification. Finally, after much hedging, Venter explained that the genomic data he gathered would be in a public database but that "probably it will belong to the nonprofit organization." So I'd be paying him to sequence my genome, but I wouldn't own the data.

annalee newitz

At the end of his lecture Venter unveiled one of the real goals of his new work. We stared at a PowerPoint slide that displayed the image of a card that looked a lot like a driver's license. Only it was issued by the "US Department of Genetic Identification," an imaginary government agency that Venter predicted would exist in the future. This agency would use the biotech Venter's lab is developing to sequence your genome on the cheap and associate its unique code with an ID card the moment you were born. In the future, not only Venter but also the government will have a chance to own your genomic data. As an aside, Venter noted that policy makers ought to create genetic antidiscrimination laws to go along with genetic identity tracking.

annalee newitz



idtrail.org

ON THE IDENTITY  
TRAIL



## plenty of eyes **at the bottom?**

nanomedicine and **the future of privacy**



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

idtrail.org

ON THE IDENTITY  
TRAIL



## **Session 3B: Current Privacy Concerns and Proposed Design Recommendations**

**Chair: Mike Gurski, Director, Privacy Center of Excellence, Bell Information and Communication Technology Solutions, Inc.**

### **Session Overview:**

This session will examine the current privacy and security architectures, models, and policies; identify current and up-coming concerns and issues; and conclude by making practical and thoughtful recommendations to navigate safely through them.

### **Biography of Chair:**

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. Gurski 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. Gurski is also a founding member of the "The Privacy Network", a knowledge exchange network to link various privacy communities in Canada.



# EHR and Privacy Enhancing Technology

Mike Gurski,  
Director: Bell Privacy Centre of Excellence

Electronic Health Information & Privacy Conference  
Ottawa, December 3, 2007

1



## Agenda.

- Setting up the Panelists



## The Questions

- **Question**
  - Has the CSA model code and its progenitors proven an efficacious for privacy protection?
- **Question**
  - What value has the PETs discourse provided?
- **Question**
  - What direction should we be heading in with the EHR?

## A Path to the Definition Answer: A Taxonomy of Privacy Violations

### Information Collection

Surveillance, Interrogation

### Information Processing

Aggregation, Identification, Insecurity,  
Secondary Use, Exclusion

**Courtesy: Daniel Solove: “I’ve got nothing to hide”  
and other misunderstandings of privacy**

## A Path to the Definition Answer: A Taxonomy of Privacy Violations

### Information Dissemination

*Breach of Confidentiality, Disclosure , Exposure, Increased Accessibility, Blackmail, Appropriation, Distortion*

### Invasion

*Intrusion, Decisional Interference*

## Results of the PETs Discourse

**Two streams.**

**The PETs of David Chaum:**

**cryptography, anonymity, mix networks,  
PETSymposium research**

**The PETs of Marc Rotenberg, John Borking et al**

**Minimize collection, processing: no longer a  
path to anonymity**

## The Clarke Taxonomy

**Privacy Invasive Technologies (PITs)** ( the membership is legion)

**Pseudo-PETs:** Trust Seals, P3P

**Counter PITs** spam-filters, cookie-managers, password managers, personal firewalls, virus protection software and spyware-sweepers

**Savage PETs** Chaum TOR, PSIPHON, Zero Knowledge Proofs

**Gentle PETs:** HIPAAT, Privacy Analytics

<http://www.anu.edu.au/people/Roger.Clarke/EC/PETsBusCase.html>

## The EHR Discussion and Privacy

**The EHR Vision:** a secure and private lifetime record of their key health history and care within the health system. The record is available electronically to authorized health providers and the individual anywhere, anytime

**The Privacy & Security Architecture 10 Services for the full Blueprint.**



# Questions?

## Contact Information

**Mike Gurski,**  
**Director: Bell Privacy Centre of Excellence**  
**905-751-4310**  
**[mike.gurski@bell.ca](mailto:mike.gurski@bell.ca)**

## **A Pragmatic Look at Privacy , Medical Practice and the EHR**

**Bill Pascal, Chief Technology Officer, Canadian Medical Association**

### **Bio:**

Mr. Pascal is the. Chief Technology Officer for the Canadian Medical Association where he has responsibility for shaping the strategic direction and policy for the CMA's e-Health agenda.

He has worked in the economic policy and social policy sectors at the Federal government level as well as run operations in regional and headquarter environments.

He has developed air, railway and marine transportation policies as well as built airports throughout the north and negotiated ferry service contracts on both coasts of Canada. He has been responsible for communications policy while at the Privy Council Office and in Health Canada. He has developed health policies and managed the Central Region operations for Health Canada which included Ontario, Manitoba and Saskatchewan. He has managed several large projects, most notably, the Federal government's involvement at Expo 86 in Vancouver and at the 1988 XV Olympic Winter Games in Calgary. Most recently he was the Director General, Office of Health and Information Highway which had responsibility for co-ordinating, facilitating and managing health infostructure-related activities both within Health Canada, with other Federal government departments, with all the provinces and territories and other stakeholders. His work led to an agreement on Information Technology investments in the health care sector in Canada with all provinces and territories and the creation of Canada Health Infoway.

He is an electrical engineer, certified management accountant and urban planner by academic training.

In 2001 he received the Lieutenant Governor's Medal of Distinction in Public Administration for his work as Chair of the Federal Council in Ontario.

# A Pragmatic Look at Privacy, Medical Practice and the EHR

William Pascal, CTO,  
Canadian Medical Association  
Electronic Health Information & Privacy Conference



## Physicians & Privacy

- Physicians take patient privacy very seriously
- Trust is cornerstone of physician-patient relationship
- Physician practice subject to strict regulatory requirements with very real consequences
- Protecting patient information is fundamental to practice



## **Issues in an Electronic Practice Environment**

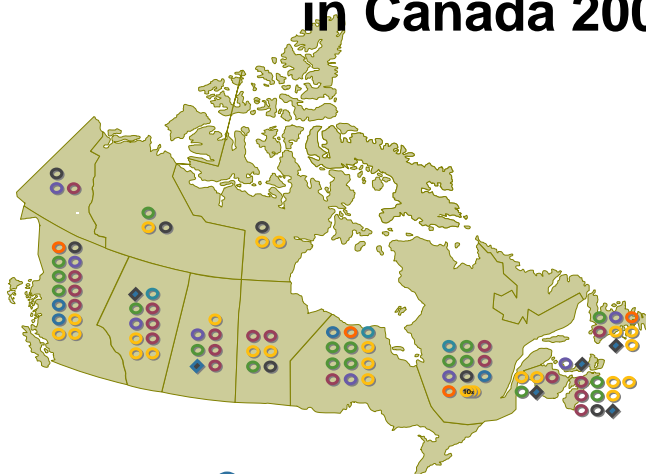
- **Many issues in paper world are heightened**
- **Privacy and business processes become interwoven**
- **Privacy more complex in e-environment**
  - **More data sharing, creation of provincial and regional dBs and ability to link data**
  - **Means more players need to think about privacy issue.**
  - **If not – risk eroding patient-physician relationship**

## **Technology Neither Policy Nor Practice Neutral**

- **Creating an e-practice environment is neither policy nor practice neutral**
- **Standards, rules and policies all impact care delivery and cost**
- **Technology influences function and policy**
- **Must take care that as we introduce new rules we clearly understand these implications – especially on privacy**



## Data Base Development in Canada 2007



- Registries
- Diagnostic Imaging
- Drug Info Systems
- Lab Info Systems
- Telehealth
- Interoperable EHR
- Public Health Surv.
- Innovation & Adoption
- Cross Program Projects

Source: Canada Health Infoway



## **Clinician Issues Going Forward**

- **It will be critical both for the physician community and policy/rule makers to manage these key issues going forward:**
  - **Ensure greater emphasis on data stewardship**
  - **Consider the provider – end-user input, needs and feedback is essential**
  - **Consider the cost – not only who pays for technology but what are “lost time” costs of undertaking new processes/requirements of an e-environment**
  - **Impact of new rules on care encounter**

## **System Issues Going Forward**

- **Provider and system liability – who is responsible/accountable when things go wrong; electronic environment and system-wide data sharing impacts physician (and other provider) liability?**
- **Privacy in larger systems – What is the relationship between data aggregation and privacy**

## Policy Issues Going Forward

- Which rules and procedures will be enforced by technology, which will be monitored by technology, and which will rely on non-technology infrastructure and the ethical and professional responsibility of those in the system
- How to manage consent for research – both in clinical trials and population health research
- How will trust and confidentiality be addressed in the new computerized systems

## A Final Thought


**“One of assumptions in the EHR business model is that the data has to move substantial distances. While the value of moving data in the local “circle of care” is increasingly obvious, it is less clear that there is a need for health information to travel out of province, or that the ability for instantaneous access to large datasets at long distances doesn’t come at the cost of other values such as autonomy and confidentiality. The largest value of a large pan-Canadian EHR system may be the advantages it provides by enforcing a standard of local interoperability”**

## **Designing Personal Information Networked Landscapes: Mirages, Quicksands and Safe Information Flow Paths Finding**

**Pierrot Peladeau, Centre for Bioethics, Clinical Research Institute of Montreal**

### **Bio:**

Specializing in social assessment of personal information systems since 1982, Pierrot Péladeau is a visiting researcher at the Centre for Bioethics of the Clinical Research Institute of Montreal (IRCM) and at Communautique, as well as an associate researcher at CEFRIO, a public knowledge transfer centre in the field of informatics and organizations. In the healthcare field, he notably acted as special advisor to the Advisory Council on Health Infostructure of the Canadian Minister of Health (1998-1999); participated in the assessment of a health smart card showcase project in Laval (Quebec) and subsequently Quebec's health smart card deployment project (2000-2002); and co-authored "Health Information Networking: Manual for the Management of Ethical and Social Issues" [March, 2004, Centre for Bioethics, IRCM].



Telehealth Ethics Programme

CENTRE FOR BIOETHICS  
ANALYSIS POLICY AND ETHICS IN HEALTH CARE

cefrio  
20 Years of Innovation through IT

COMMUNAUTIQUE

## Designing Personal Information Networked Landscapes: Mirages, Quicksands and Safe Information Flow Paths Finding

Pierrot Péladeau  
pierrot.peladeau@ircm.qc.ca  
<http://persons-information-pierrotpeladeau.blogspot.com>

Electronic Health Information & Privacy Conference  
Ottawa, December 3, 2007



Telehealth Ethics Programme

CENTRE FOR BIOETHICS  
ANALYSIS POLICY AND ETHICS IN HEALTH CARE

cefrio  
20 Years of Innovation through IT

COMMUNAUTIQUE

## From the Personal Information System Assessment Perspective

### Notion of “Privacy Enhancing Technology”:

- Confusing at best
- Often worthless and even harmful

Telehealth Ethics Programme
CENTRE FOR BIOETHICS
cefrío
COMMUNAUTIQUE

## From the Personal Information System Assessment Perspective

**Notion of “Design”:**

- Informatics is efficient regulation of interpersonal interactions
- Issue is less a matter of architecture or modeling that of governance and structures of communication, coordination and collaboration

Telehealth Ethics Programme
CENTRE FOR BIOETHICS
cefrío
COMMUNAUTIQUE

## Visual Models

**Prevention of illegal access to prescription drugs:**

- DATA MODELS

```

graph LR
    Patient[Patient] --- HealthProfessional[Health Professional]
  
```

The diagram illustrates a data model for preventing illegal access to prescription drugs. It features two rounded rectangular boxes: one labeled 'Patient' on the left and one labeled 'Health Professional' on the right. These two boxes are connected by a horizontal line, representing the interaction or data flow between the patient and the healthcare provider.

Telehealth Ethics Programme

BIOETHICS

cefrio

COMMUNAUTIQUE

## Visual Models

**Prevention of illegal access to prescription drugs:**

- DATA MODELS
- USER CASES

```

graph TD
    Patient[Patient] --- HP[Health Professional]
    subgraph Warning
        HP2[Health Professional] --- GOP[Group of professionals]
    end
  
```

Telehealth Ethics Programme

BIOETHICS

cefrio

COMMUNAUTIQUE

## Visual Models

**Prevention of illegal access to prescription drugs:**

- DATA MODELS
- USER CASES
- SOCIAL MODEL

```

graph TD
    Patient[Patient] --- HP[Health Professional]
    subgraph Warning
        HP2[Health Professional] --- GOP[Group of professionals]
    end
    subgraph Detection
        SP[Suspect or presumed guilty] <--> AD[Agent of detection & prevention of infractions]
    end
  
```

Telehealth Ethics Programme

CENTRE FOR BIOETHICS  
ANALYSIS POLICY AND ETHICS IN HEALTHCARE

cefrio  
20 Years of Innovation through IT

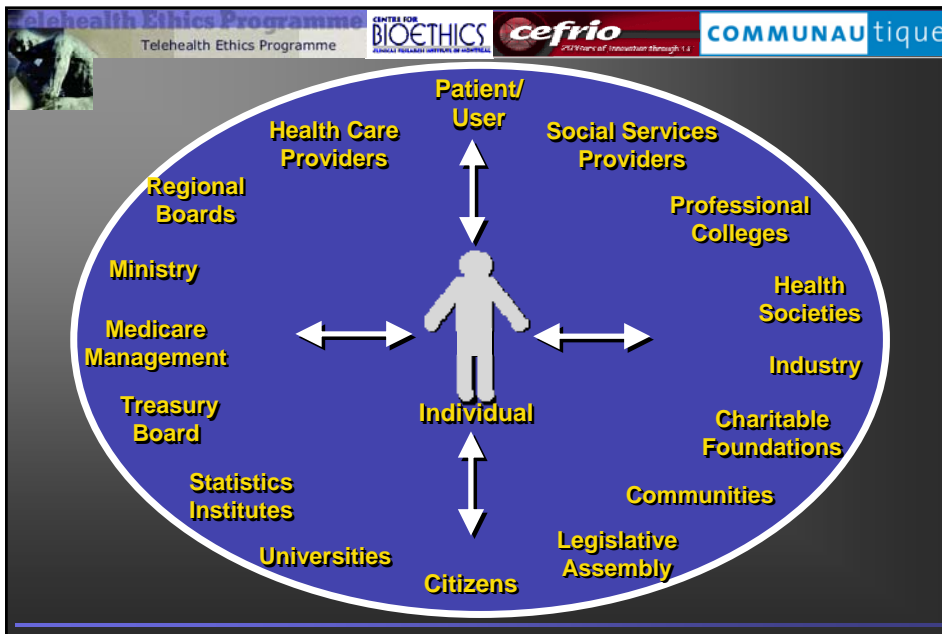
COMMUNAUTIQUE

## Common Assumptions about Personal Information Networking


- “data” have universal usefulness
- thus data are a precious “resource”
- “silos” prevent benefit from resource
- “privacy enhancing” designs help dissolve silos







Telehealth Ethics Programme    CENTRE FOR **BIOETHICS**    20 Years of Innovation through IT **cefrío**    **COMMUNAU**tique




## Personal Information Networking

**Conditions for success:**

- looking beyond abstractions
- understanding real-life human interactions, pragmatics and corresponding stakes and issues

Telehealth Ethics Programme    CENTRE FOR **BIOETHICS**    20 Years of Innovation through IT **cefrío**    **COMMUNAU**tique



## Designing Personal Information Networked Landscapes:

# Mirages, Quicksands and Safe Information Flow Paths Finding

Pierrot Péladeau  
pierrot.peladeau@ircm.qc.ca  
<http://persons-information-pierrotpeladeau.blogspot.com>

Electronic Health Information & Privacy Conference  
Ottawa, December 3, 2007

Programme Éthique et  
Télesanté

CENTRE DE  
BIOÉTHIQUE  
INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL

cefrío  
10 ans d'innovation par le ST

COMMUNAU  
tique

**Design des espaces  
d'informations personnelles réseautées :**

**Mirages, sables mouvants  
et trajets sûrs  
pour flux d'informations**

Pierrot Péladeau  
pierrot.peladeau@ircm.qc.ca  
<http://information-personnes-pierrotpeladeau.blogspot.com/>

Electronic Health Information & Privacy Conference  
Ottawa, 3 décembre, 2007

Programme Éthique et  
Télesanté

CENTRE DE  
BIOÉTHIQUE  
INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL

cefrío  
10 ans d'innovation par le ST

COMMUNAU  
tique

**Du point de vue de l'évaluation de systèmes  
d'information sur les personnes**

**Notion de « *Privacy Enhancing Technology* » :**

- Confuse au mieux
- Souvent inutile et même nuisible

Programme Éthique et  
Télesanté

CÉNTRE DE  
BIOÉTHIQUE  
INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL

**cefrio**  
10 ans d'innovation par le ST

COMMUNAU  
tique

## Du point de vue de l'évaluation de systèmes d'information sur les personnes

**Notion de « Design » :**

- Informatique est une forme efficace de régulation des interactions interpersonnelles
- Questions moins liées à l'architecture ou au modèle qu'à la gouvernance et aux structures de communication, coordination et collaboration

Programme Éthique et  
Télesanté

CÉNTRE DE  
BIOÉTHIQUE  
INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL

**cefrio**  
10 ans d'innovation par le ST

COMMUNAU  
tique

## Modèles visuels

**SI Prévention de l'accès illégal aux médicaments :**

- MODÈLE DE DONNÉES

```

graph LR
    Patient[Patient] --- Professionnel[Professionnel de la santé]
  
```

Programme Éthique et Télésanté

CENTRE DE BIOÉTHIQUE  
INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL

cefrio  
10 ans d'innovation par le DT

COMMUNAUTIQUE

## Modèles visuels

**SI Prévention de l'accès illégal aux médicaments :**

- MODÈLE DE DONNÉES
- CAS D'UTILISATION

The diagram illustrates the 'Modèle de données' (Data Model) and 'Cas d'utilisation' (Case Use) for preventing illegal access to drugs. It features two main components: a box diagram at the top and a stick figure diagram at the bottom. The box diagram shows a 'Patient' box connected to a 'Professionnel de la santé' box. The stick figure diagram shows a 'Professionnel de la santé' stick figure connected to a 'Groupe de professionnels' stick figure, with an oval labeled 'Avertissement' (Warning) between them.

Programme Éthique et Télésanté

CENTRE DE BIOÉTHIQUE  
INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL

cefrio  
10 ans d'innovation par le DT

COMMUNAUTIQUE

## Modèles visuels

**SI Prévention de l'accès illégal aux médicaments :**

- MODÈLE DE DONNÉES
- CAS D'UTILISATION
- MODÈLE SOCIAL

The diagram illustrates the 'Modèle de données' (Data Model), 'Cas d'utilisation' (Case Use), and 'Modèle social' (Social Model) for preventing illegal access to drugs. It features three main components: a box diagram at the top, a stick figure diagram in the middle, and a stick figure diagram at the bottom. The box diagram shows a 'Patient' box connected to a 'Professionnel de la santé' box. The middle stick figure diagram shows a 'Professionnel de la santé' stick figure connected to a 'Groupe de professionnels' stick figure, with an oval labeled 'Avertissement' (Warning) between them. The bottom stick figure diagram shows a 'Suspect ou présumé coupable' stick figure connected to an 'Agent de détection et prévention d'infractions' stick figure, with a double-headed arrow labeled 'Détection et prévention d'infractions' (Detection and prevention of infractions) between them.

CENTRE DE

BIOÉTHIQUE

INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL

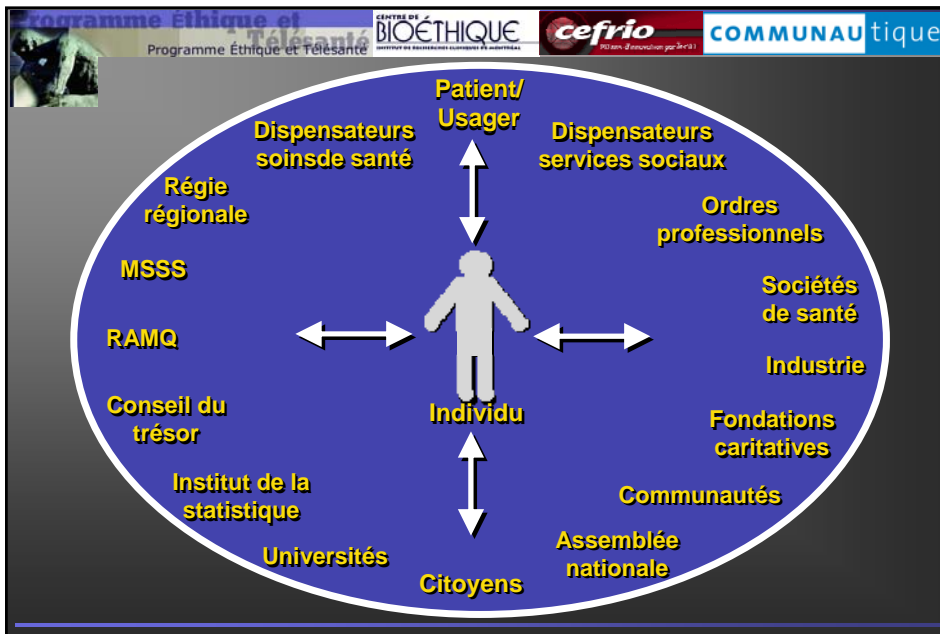
COMMUNAU


tique

## Suppositions courantes du réseautage d'informations personnelles

- « données » ont une utilité universelle
- données sont donc une « ressource » précieuse
- « silos » font obstacle aux bénéfices de la ressource
- designs de type « *privacy enhancing* » aident à dissoudre les silos








**Programme Éthique et**  
**Télé santé**  
Programme Éthique et Télé santé

CENTRE DE  
**BIOÉTHIQUE**  
INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL



**cefrio**  
10 ans d'innovation par le ST

**COMMUNAU**tique

## Réseautage d'informations personnelles

**Conditions de succès :**

- regarder par delà les abstractions
- comprendre les interactions humaines réelles, leur pragmatique et les enjeux et questions liées



**Programme Éthique et**  
**Télé santé**  
Programme Éthique et Télé santé

CENTRE DE  
**BIOÉTHIQUE**  
INSTITUT DE RECHERCHES CLINIQUES DE MONTRÉAL



**cefrio**  
10 ans d'innovation par le ST

**COMMUNAU**tique

**Design des espaces  
d'informations personnelles réseautées :**

## Mirages, sables mouvants et trajets sûrs pour flux d'informations

**Pierrot Péladeau**  
 pierrot.peladeau@ircm.qc.ca  
<http://information-personnes-pierrotpeladeau.blogspot.com>

**Electronic Health Information & Privacy Conference**  
 Ottawa, 3 décembre, 2007



## **So Who Wants to Know? Research Access to E.H.R. Data**

### **Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada**

#### **Bio:**

Patricia Kosseim is General Counsel at the Office of the Privacy Commissioner of Canada (OPC) since January 2005. She provides legal and policy advice on privacy issues that arise in both the public and private sectors; she represents OPC before Federal Courts and Parliamentary Committees; directs legal research on emerging privacy issues; and works collaboratively with stakeholders across multiple jurisdictions and sectors.

Before joining OPC, Patricia spent five years at the Ethics Office of the Canadian Institutes of Health Research leading major research and policy initiatives to address ethical/legal/social issues related to health research. During this period, she was briefly seconded to Canada Health Infoway Inc. to advise on legal issues related to the development of pan-Canadian electronic health record systems. Prior to this, Patricia practiced in Montreal for over six years with a major national law firm in areas of human rights, health law, labor and employment law, administrative law and professional regulation/liability.

Patricia was called to the Québec Bar in 1993. She holds degrees in Business (B.Com '87) and Laws (B.C.L. / LL.B. '92) from McGill University, as well as a Master's Degree in Medical Law and Ethics (M.A.'94) from King's College in London, U.K.

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.

### **Megan Brady, Legal Counsel, Office of the Privacy Commissioner of Canada**

#### **Bio:**

Megan Brady is Legal Counsel with the Office of the Privacy Commissioner of Canada. Prior to joining the Office of the Privacy Commissioner of Canada, Megan Brady served as law clerk to the Honourable Justice Rosalie Abella at the Supreme Court of Canada and was called to the Ontario bar in 2006. Megan obtained a law degree from the University of Ottawa Faculty of Law after earning two Master's degrees from Queen's University at Kingston, the first in philosophy (M.A.) and the second in public administration (MPA). She has worked as a policy analyst with the federal and provincial governments in the fields of charity and health policy and has also served as a research assistant to a well-known constitutional and administrative law expert at the University of Ottawa.

## So Who Wants to Know? Research Access to E.H.R. Data



Patricia Kosseim and Megan Brady  
Electronic Health Information & Privacy Conference  
National Arts Centre, Ottawa, Canada  
December 3, 2007



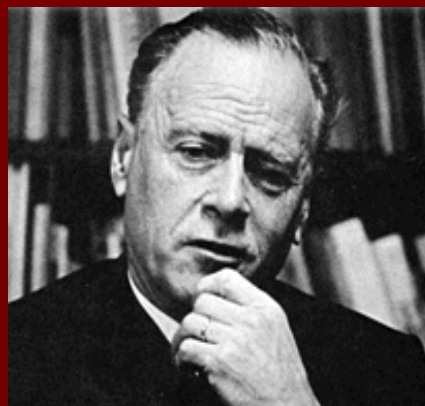
Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada

## General Overview of the Issue

- We shape our tools  
and afterwards our  
tools shape us.

- *Marshall McLuhan*



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada

## General Overview of the Issue

- The medium is the message. This is merely to say that the personal and social consequences of any medium - that is, of any extension of ourselves - result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology.



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada

## Historical Background



- The incremental deployment of EHRs has focused on enabling the primary use of health care, leaving potential research uses in legal and ethical "limbo"

# The "Consent Issue": Policy Options

- Specific informed consent
- Broad Consent
- Consent Exemptions
- Retrospective Legislative Solutions
- Reconceptualizing Research



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada



**Commissariat  
à la protection de  
la vie privée du Canada**

[illegible]

**Commissariat  
à la protection de  
la vie privée du Canada**

# Broad Consent



Office of the  
Privacy Commissioner  
of Canada

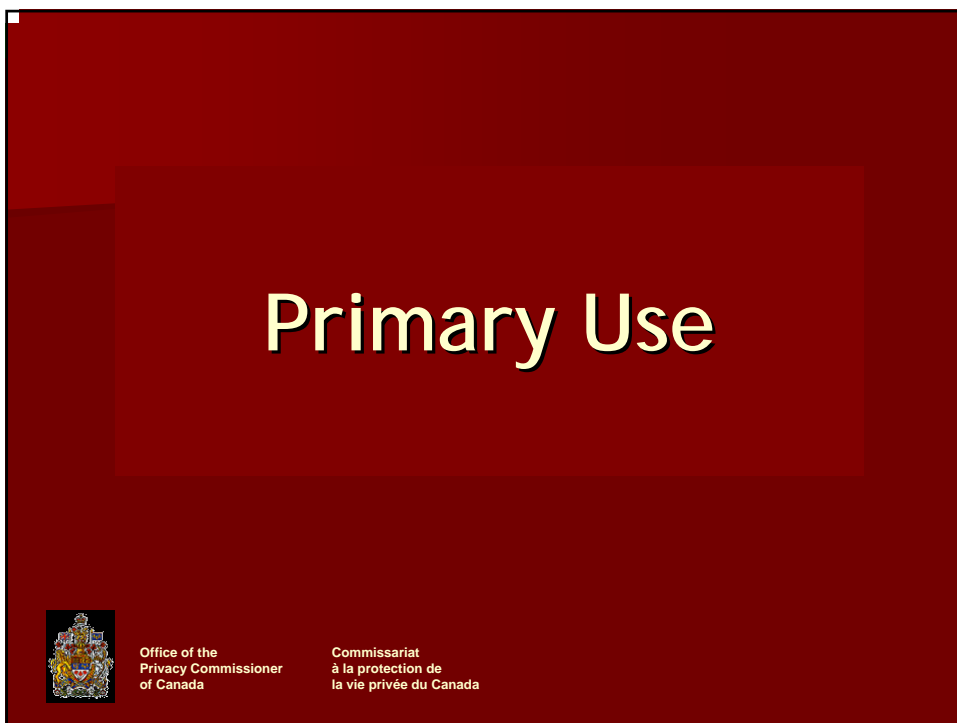
Commissariat  
à la protection de  
la vie privée du Canada

# Informed Consent



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada



# Conclusions

We drive into the future using only  
our rearview mirror.

- *Marshall McLuhan*



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada

# Thank you / Merci



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada