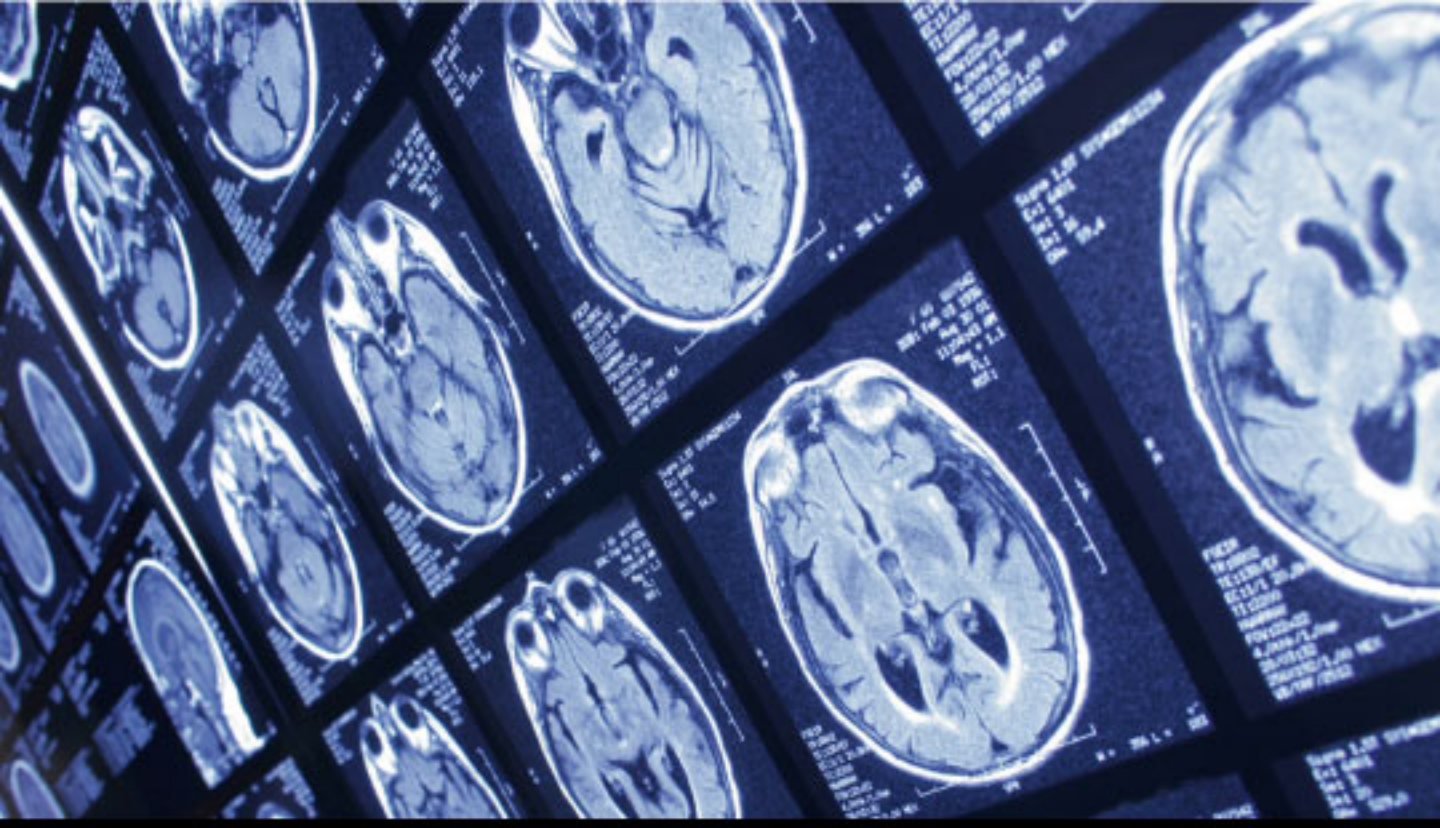


2008 Electronic Health Information & Privacy Conference

November 3, 2008 - Ottawa, Canada

Sponsored by:

Microsoft

PRIVACY ANALYTICS

Supported by:

Public Health Agency of Canada / Agence de la santé publique du Canada

CAPAPA

COACH

htx.ca The Health Technology Exchange

OCRI

www.ehip.ca

PROGRAM

REGISTRATION & WELCOME (8:00 – 8:30)

OPENING REMARKS & PLENARY (8:30 – 9:45)

Ballrooms A & B

Joe Pendleton, Director of the Special Investigations Unit, Government of Alberta
"The Growing Threat of Medical Identity Theft in Canada"

BREAK (9:45 – 10:15)

TRACK 1

Ballroom D

PANEL 1A (10:15 – 12:00)

PRIVACY VS. PUBLIC HEALTH?

Session Chair: Philip Abdelmalik, Public Health Agency of Canada

Panelists:

Cory Neudorf, Chief Medical Health Officer, Saskatoon Regional Health Authority

Dr. Kumanan Wilson, Associate Professor, University of Ottawa

Dr. Gregory Taylor, Director General, Office of Public Health Practice, Public Health Agency of Canada

Philippa Lawson, Executive Director, CIPPIC, Univeristy of Ottawa

TRACK 2

Ballroom C

SESSION 2A (10:15 – 12:00)

PRIVACY IN PRACTICE

Session Chair: Michael Power, eHealth Ontario

Presenters:

Sasha Romanosky, PhD Student, Carnegie Mellon University

David McKie, Investigative Reporter, CBC News

Elaine Sawatsky, Privacy Consultant & Co-presenter Ognjenka Djurdjev, Corporate Director Decision Support, Provincial Health Services Authority, British Columbia

LUNCH (12:00 – 13:00)

Ballrooms A & B

SESSION 1B (13:00 – 14:45)

LOCATION PRIVACY

Session Chair: David Buckeridge, McGill University

Presenters:

Christopher Cassa, Harvard-MIT Division of Health Sciences and Technology

SESSION 2B (13:00 – 14:45)

PRIVACY LAW

Session Chair: Murray Long, Murray Long & Associates Inc.

Presenters:

Ross Hodgins, Office of the Information Commissioner

Michael Leitner, Department of Geography and Anthropology, Louisiana State University	Teresa Scassa, Canada Research Chair in Information Law, Faculty of Law, University of Ottawa
Khaled El Emam, CHEO Research Institute and University of Ottawa	Carol Appathurai, Director of PHIPA Review Project, Ministry of Health and Long Term Care
BREAK (14:45 – 15:15)	
SESSION 1C (15:15 – 17:00) **SECONDARY USE AND POPULATION REGISTRIES** **Session Chair: Mike Gurski, Bell Canada Privacy Centre of Excellence**	**SESSION 2C** (15:15 – 17:00) **PERSONAL HEALTH RECORDS** **Session Chair: Bradley Malin, Vanderbilt University**
Presenters: Patricia Kosseim, GE3LS Officer, Genome Canada	**Presenters:** George Scriban, Senior Global Strategist, Microsoft Corporation
Dr. Jim Bottomley, Director of the Ontario Perinatal Surveillance System	Kevin J. Leonard, Associate Professor, University of Toronto
Regis Vaillancourt, Director of Pharmacy, & Co-presenter Tyson Roffey, CIO, Children's Hospital of Eastern Ontario	Ben Heywood, Co-founder & President, PatientsLikeMe

Table of Contents

Introduction

2008 Electronic Health and Information Privacy Conference

More and more health information is being collected about us - and much of that data is collected, transmitted and stored electronically.

There is increasing demand to use this personal health information for research, administrative, and policy making purposes. At the same time, the number of privacy breaches is rising. This has multiple negative consequences: from reducing the trust of patients in the public and private organizations that manage their personal information, to patients adopting privacy protective behaviors that may be detrimental to their well being.

Continuing on the previous three years' events, the 2008 conference will address emerging themes that have become more relevant over the last year. We will focus on public health uses of personal health information, location privacy, recent court cases that help define what is personal information, privacy of DNA databases, and privacy enhancing technologies.

Khaled El Emam, University of Ottawa
Philip AbdelMalik, Public Health Agency of Canada
and David Buckeridge, McGill University
Organizing Committee

The Growing Threat of Medical Identity Theft in Canada

Keynote Speaker: Joe Pendleton, Director of the Special Investigations Unit, Government of Alberta

Abstract:

On the 15 of July 1975, a Manitoba family lost their lives in a tragic automobile collision near the town of Princeton in British Columbia. Peter and Lillian Klassen were on vacation with their four children, Randy (10 yrs), brother Leslie (15) and sisters Cheryl (16) and Laureen (14) when their lives ended that day.

On the 1st of August 2001, twenty-six years later, a male was released from a Calgary hospital after undergoing successful surgery to treat a lifestyle inflicted injury. Still bandaged, he took a cab to the Calgary International airport to catch a flight to his native San Francisco.

Thirty-nine year old William Martin Skupowski had immigration warrants outstanding for his arrest in Canada as well as arrest warrants in California for marijuana cultivation. Mr. Skupowski was not afraid of being apprehended as he passed through American Customs. Skupowski was cloaked in the identity of deceased 10 year old Randy Klassen. The mechanism that had provided Skupowski virtually free medical care was now about to ensure a safe return to his American home.

Joe Pendleton will present this case study, providing an informative look at how various forms of identity fraud are committed in Canada. This particular example will reveal how easily Canadian health care benefits can be compromised, and how medical privacy laws and culture make detection and prosecution extremely difficult for law enforcement.

Bio:

Joe Pendleton is the Director of Special Investigations within Service Alberta and was instrumental in establishing the permanent investigative unit. The Special Investigations Unit (SIU) provides registry-related oversight and investigative services, facial recognition analysis and investigation, court certificates and covert programs. Joe's unit also provides investigative and forensic support to other Alberta ministries that includes privacy breach investigation and mitigation. Joe is currently on loan to the Province of Manitoba to assist them in implementing facial recognition and establishing their own investigative unit.

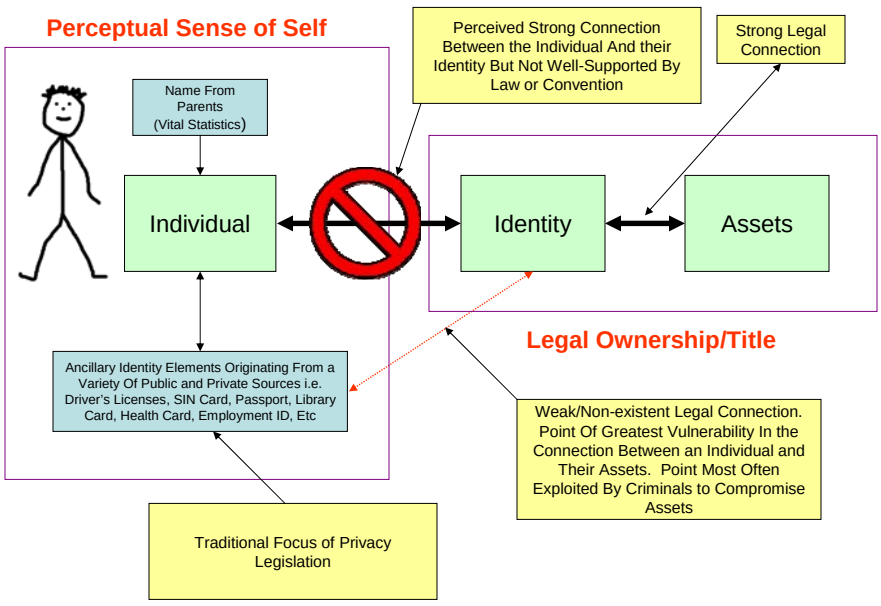
Joe earned his extensive knowledge of identity theft and economic crime during his years with the Edmonton Police Service. While serving, he was awarded the Weber SEAVEY award (the world's top policing award) for work relating to Edmonton's Community Based Policing initiative.

Joe has spoken across the country to numerous privacy and industry groups about Identity Crime and privacy issues.

HEALTH CARE FRAUD
A CASE STUDY

Joe Pendleton
Sterling Corporate Security and
Information Integrity Group
www.sterlingsecurity.ca

Functioning Social Relationship Between "Self" – "Identity" – "Assets"

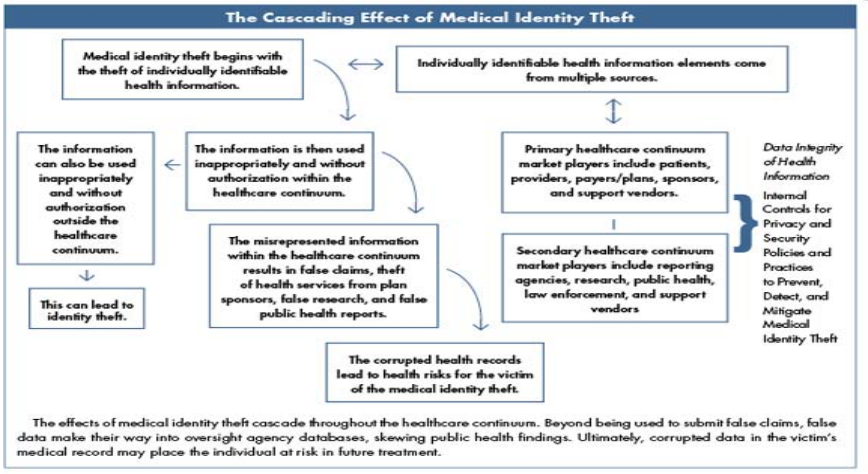


Who's The Victim?

- In fraud investigations generally the rule is "Follow the Money". This is also true when determining who is the "Complainant".
- As in most Identity Fraud, the actual identity holder is seldom the Complainant.
- The police will not pursue a complaint without a motivated and cooperative Complainant.

Fraud…Privacy….&….Medicine

Medical Identity Theft



Source: American Health Information Management Association

Issues

- Medical Identity Theft accounts for about 3% of the overall Identity Theft reported to the FTC in 2005.
- According to The Identity Theft Resource Center, the health sector is responsible for14.9% of data breaches so far in 2008. (Up from 13% in 2006)
- Personal Health Information is generally not available to police without a warrant.

PHIPA Policy # 8-05

College of Physicians and Surgeons Of Ontario

Disclosure to Police

- It is not mandatory for physicians to provide confidential material to the police in the absence of a legal obligation. At these times, the general rules regarding consent and disclosure apply, meaning that express consent, either from the patient directly, or the substitute decision-maker, will be required before the police are provided with personal health information.
- When personal health information is disclosed to the police, physicians are encouraged to record the officer's name and badge number, the request for information, the information provided, and the authority for the disclosure (e.g., consent, reporting obligation, search warrant or summons). A photocopy of any search warrant or summons should be included in the patient's medical record. The police or Crown attorney will usually take the originals but leave the physician with copies of the record so that ongoing care can be given.

Big Deal…Get A Warrant!

- In Canadian Criminal Law, There are Property Warrants, General Warrants, Production Orders, Warrants to Intercept Private Communications and Blood Warrants
- The Warrants themselves are not a problem but drafting the Informations To Obtain (ITO) those warrants are generally significant and daunting undertakings

The Start

- W.E.B. was arrested on 99 Aug 09 in Edmonton. A search warrant was conducted on his apartment as a result of an unrelated investigation. The resulting search revealed a suitcase containing thousands of documents including research on 1,806 deceased Canadians

The "Stash"

- Two hundred and Seventy-eight (278) pieces of actual identification were found among the exhibits seized representing identification in the names of 83 people.
- Complete identity packages that included SIN cards, driver's licences, health care cards and Canadian passports had been produced some of which were eventually linked to international organized criminals and members of Outlaw Motorcycle Gangs.
- The Criminals had paid up to $37,000 dollars for the identity packages.

Method Of Investigation

- The entire list of 1806 names was provided to a wide range of provincial and federal agencies who searched their databases for activity against the names.
- W.E.B.'s previous criminal activity involving over $2 Million dollars in benefits fraud was revealed.
- Application documents submitted by W.E.B. for birth certificates, SIN cards, passports and driver's licences were requested.
- Forensic attempts were made to link these applications to W.E.B. forensically as well as by association to phone numbers, stand alone voice mail boxes, proxy mail box addresses and associates.

Anatomy Of W.E.B.'s Modus Operandi

- Attend libraries and museums to conduct research on children who died in the early 1960's and 1970's who were born in one jurisdiction but died in another. (*Determine Mother's maiden name from family information on the obituaries*).
- Attend the cemeteries to harvest the subjects date of birth from their headstones.
- Contact relatives by phone for additional information or to clarify inconsistencies.
- Use the information to make written application for a birth certificate.
- All phone numbers were cell phones and stand alone voice mail boxes in alias names. All addresses were rented post boxes.

An Identity In Common

- An Alberta family was vacationing in British Columbia in the 1970's when a motorboat carrying their 12 year old son caught fire. The boy jumped into the water and drowned.
- W.E.B. produced a complete identity package using the boy's information and sold it to an International Drug Smuggler, M.I.. The forged documents were seized from M.I. by police in Germany in 1997 following M.I. 's arrest for Fraud offenses.

Pulling The Thread On a Sweater

- When the investigation requested the fraudulent applications for the boy's birth certificate, three applications were turned over. Two of them had nothing to do with W.E.B.!
- One had been mailed to a non-existent suite in a Calgary condominium complex.
- One had been mailed to a rented mailbox on Hastings Street in Vancouver.

W.E.B. Identity Spin Off Investigations

- **D.M.** (Calgary A.B.) 3 identities
- **B.W.** (New Westminster B.C.) 28 identities
- **B.T.** (Vancouver B.C.) 9 identities including a passport
- **T.S.** (Vancouver B.C., 2 identities)
- **P.W.** (Halifax N.S.) 2 identities including a passport
- **R.B.** (Coquitlam B.C.) 2 Identities confirmed several more suspected
- **A.S.** (Edmonton, Vancouver) 2 identities
- **R.M.C.** (Calgary**,** Vancouver) four identities
- **E.D.** (Edmonton) one identity including a passport
- **R.F.** (International) 7 Identities American and Canadian Passports
- **W.M.S.** (San Francisco) 2 Identities, Alberta Health Care, passports DL's and Id Cards

Mr. K

- All five members of the K family from Manitoba were vacationing in British Columbia when they were killed in a motor vehicle collision at Princeton B.C. on 75 Jul 15.
- When asked if they had ever sent a birth certificate to the Hastings Street Address, Manitoba Vital Statistics indicated that they had issued a certificate to that address on 97 Sep 24.

Tracking Mr. K

- He had obtained provincial health insurance which was in collections
- A SIN card issued for Mr. K by HRDC in December of 1997
- A British Columbia ID card was issued for Mr. K in October of 1997
- Mr. K obtained an Alberta Operator's licence in June of 2000
- A credit card from an American bank was issued in April of 2001
- A Canadian passport was granted on the 16th of May 2001

Hot On The Trail Of The Elusive Mr. K!

- A woman at a "real" Calgary address associated to Mr. K was interviewed. She claimed that he had boarded with her from "time to time" but that she didn't know him well and could not provide any further assistance.
- The Alberta lawyer who had served as the guarantor on the Mr. K passport was interviewed. She claimed to have known him for the required two years as "Mr. K" and then she "lawyered-up" right away refusing to provide additional details or information.

New York, New York!

- An credit history revealed a credit card account with a New York based bank.
- I contacted the bank in New York and established a relationship with one of their security representatives.
- Problem was…the card hadn't been used.
- She promised me that she would "drop a dime" if the card became active.

The Big "Break"!

- I was sitting having lunch at my desk on the 1st of August 2001 when my phone rang.
- My Home Trust New York bank Security Rep told me that a ticket to San Francisco had been purchased at the Calgary International Airport on the fraudulent Mr. K credit card and the plane was departing in 30 minutes!

Gotcha!

- With the assistance of U.S. Border Protection Staff and the Calgary Police Service Airport Detail, W.M.S. was arrested from his seat on the U.S. bound aircraft and turned over to a Calgary RCMP Immigration and Passport detective.
- W.M.S. was subsequently “identified” as an American citizen with outstanding warrants for his arrest in California for marijuana cultivation.

The Interview

- I interviewed W.M.S. in Calgary following his arrest.
- He said was returning home to San Francisco following surgery to correct an anal fistula.
- Although W.M.S. would provide no details he stated that this was a well-known and common strategy for San Francisco homosexuals who had no health insurance but required medical treatment for lifestyle-related afflictions.

- I contacted the health care plan who refused to make a complaint or provide any information on “Mr. K’s” case citing the Health Information Privacy Act.
- Although I prepared arrest reports recommending several serious charges against W.M.S. he was only ever convicted of Passport Fraud, sentenced to 14 days, and deported to the U.S.

Other Examples of Medical Identity Theft Not Pursued

- A doctor at a hospital treats a woman who is visiting from the Middle East and subsequently directs a hospital clerk to associate the treatment to her Canadian relative’s health account/file. The hospital later indicates that this was simply a “mistake”.
- A woman obtaining medical treatment as the result of complications from breast augmentation co opts her sister’s identity because she has no subsisting health insurance. The hospital continues to provide ongoing medical treatment under the wrong account.

My Conclusions

- There is no resolve within the existing paradigm to address medical identity fraud in Canada.
- That Health Information Privacy legislation often provides a welcome and convenient firewall to prevent or frustrate benefit-related medical frauds.

Solutions

- Be aware of the magnitude and cost of this problem.
- Do not become part of the problem by going down the “slippery slope” yourselves!
- Report medical fraud when you encounter or suspect it.
- Lobby your professional associations and politicians to allow the free flow of information to police in circumstances where there is evidence of medical fraud.

THANK YOU!

Questions?

Panel 1A: Privacy vs. Public Health?

Panel Chair: Philip AbdelMalik, Public Health Agency of Canada

Panel Description:

Public Health is defined as the organized efforts of society to keep people healthy and prevent injury, illness and premature death. It is a combination of programs, services and policies that protect and promote the health of all Canadians.

The definition of "Public Health", as given by the Chief Public Health Officer of Canada in his report released earlier this year, highlights the significant role of protecting and improving the health status of the public. This "combination of programs, services and policies" on a nation-wide level necessitates data and information flow within and between networks and jurisdictions, merging clinical data with public health methods, analyses and interpretation. Given the electronic age in which we live, this should, in theory, be a cinch! However, concerns over data privacy, confidentiality and security must also be taken into consideration when collecting, storing, using, sharing and disseminating data. While this may not be the only potential barrier to effective public health practice, it is certainly one that requires serious attention.

On the one hand, failure to adequately protect privacy can lead to a reduction in public trust, which can be detrimental to an individual's well-being, and inhibiting to public health activities. On the other hand, strict policies that prioritize privacy can fetter public health activities such that they become ineffective in fulfilling their role.

In this session, the role of privacy in public health will be explored, along with the balance required for public health to fulfill its mandate.

Bio of Chair:

Philip AbdelMalik is currently the Acting Manager of the GIS Infrastructure at the Public Health Agency of Canada's Office of Public Health Practice (normally, he wears an "Epidemiologist and Senior GIS Analyst" hat). Prior to joining the Agency, Philip was a research coordinator at the Clinical Genetics Research Program, at the University of Toronto / Centre of Addiction and Mental Health, where his work focused on the epidemiology and genetics of schizophrenia, particularly in relation to head trauma. Since joining the Agency in May of 2004, Philip's primary research focus has been the use and promotion of GIS in epidemiology and public health, with particular emphasis on issues of location-privacy. Philip completed his M.H.Sc. in Community Health and Epidemiology at the University of Toronto, and is currently a Ph.D. candidate in Public Health Informatics at the Peninsula Postgraduate Health Institute in the UK.

Privacy and Public Health: Pathways & Pitfalls

Dr. Cordell Neudorf, Chief Medical Health Officer, Saskatoon Health Region

Bio:

Dr. Neudorf is the Chief Medical Health Officer for the Saskatoon Health Region. He received his medical degree from the University of Saskatchewan, a Master's of Health Science degree in Community Health and Epidemiology from the University of Toronto, and is a fellow of the Royal College of Physicians and Surgeons of Canada with Certification in the specialty of Community Medicine. He is the past president of the National Specialty Society for Community Medicine, Chair-elect of the Canadian Public Health Association, and Chair of the Canadian Population Health Initiative Council.

Dr. Neudorf is a Clinical Associate Professor in the Department of Community Health and Epidemiology at the University of Saskatchewan, College of Medicine.

His research interests include Health Inequalities, health status indicators and surveys, Health status monitoring and reporting, and integrating Population Health data and Geographic Information Systems into public health and health planning.

Privacy and Public Health:
Pathways and Pitfalls

Panel Discussion

Electronic Health Information and Privacy Conference

Dr. Cory Neudorf, Chief Medical Health Officer
Saskatoon Health Region

Public Health Practise and Privacy Issues

- Surveillance is a core service and critical tool for public health practise but is often misunderstood by privacy officers as an intrusion of an individual's privacy or being merely an academic exercise.
- It is difficult to interpret privacy legislation written from an individualist, protectionist perspective (e.g. physician trustees and individual patient records) in the light of population or public health, where the population is the patient and the needs of the many often trump the needs of the few (outbreak management, immunization coverage needs, disease control, health protection).
- In addition to standard public health practise data needs, Public Health is taking on a role as population health data provider and interpreter to the health system or the greater human service sector for system planning and prioritizing in light of greater understanding about the determinants of health

Levels of data sharing needed at the RHA level

1. **De-identified, high level aggregate** data
   E.g. Indicators at regional level: Service utilization, Health Status Report, System Performance & Outcomes for broad monitoring and comparisons
2. **De-identified low level aggregate data**
   E.g. Indicators at sub-regional level for prioritization and program planning / policy making (CCIS)
3. **De-identified, individual records**
   E.g. Utilization Reviews and audits, surveillance,
4. **Identifiable, individual records**
   E.g. Case Management, shared service delivery, Communicable Disease control

Example 1

- **Case Study – Complex Needs Protocol**
  - **Needs Individual level data**
  - **Process:**
    - **Obtain parental / student consent**
    - **Share only the information necessary to cooperate on care (HIPA sec. 23) disclosure on "need to know" basis**
      - **E.g. Mental Health - the behavioural or cognitive issues associated with the condition, but not necessarily the details of the diagnosis**
      - **E.g. Infectious Disease – what precautions are necessary for safety, but not the name of the specific disease**
    - **Share more details only if situation changes**
      - **E.g. if precautions were not followed and there is a need for contact tracing (such as an at risk exposure to blood from an HIV +'ve source) PHA (1994)sec 35**
    - **NOTE: PHA is exempted from certain sections of HIPA (II, IV, V) (collection, use, disclosure and access to data) HIPA sec 4(4)g**

Example 2

- STI Contact tracing
  - Person with infectious disease but has limited information about their contacts (first name, school and class they are in) no last name, no address
  - PHA (1994) sec 35 gives authority for tracking down contacts for purposes of treatment and to prevent further spread
  - Work with school to help identify individual (PHA sec 65 (1,2)), (HIPA part IV sec 27 (4) l, m)council them and encourage them to involve parent/guardian in decisions, but treatment is primary concern if person is competent to make own decisions. If orders under the PHA are required and person is under age 14, parents need to be informed. (PHA sec 39)

Example 3 -

- Health system needs listing of students and health numbers from Education (HIPA sec 20, 27) Disclosure from one trustee to another
  - E.g. Mass Immunization program
- Education needs listing of numbers of students of a certain age from Health (HIPA sec 23) minimum personal information required to serve the purpose, yet assist in cutting down administrative overhead between Departments)
  - E.g. Enrolment planning

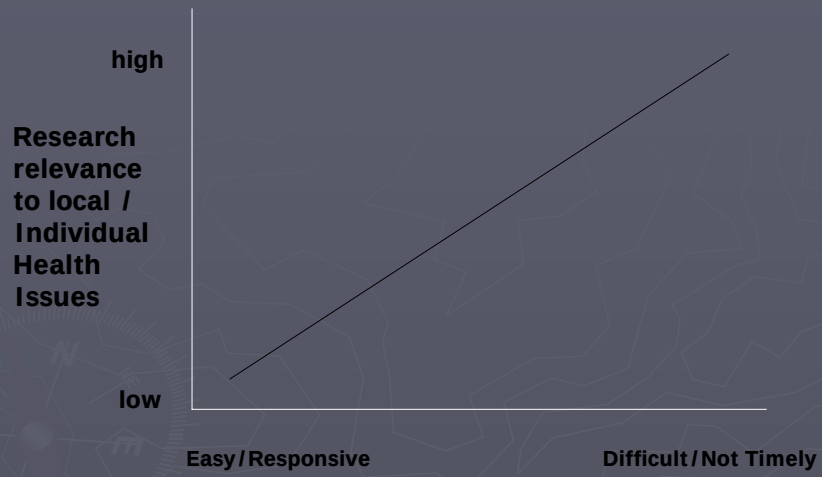
Example 4

- CCIS data
  - **Intended Users**- Management, politicians, clinicians, and researchers
  - **Intended purpose**- Population health priorities and planning, management, community profiles, intersectoral work on determinants of health
  - **Dissemination plan** – National data releases, with some free access to high level aggregate data, with cost recovery for custom table generation. Limited data sharing allowed
  - **Challenges and Opportunities-** legislation issues for data created by linking existing other data; need for data suppression if linking data could still result in identification of an individual. (Otherwise HIPA sec 3 (2)a applies and allows for this type of sharing

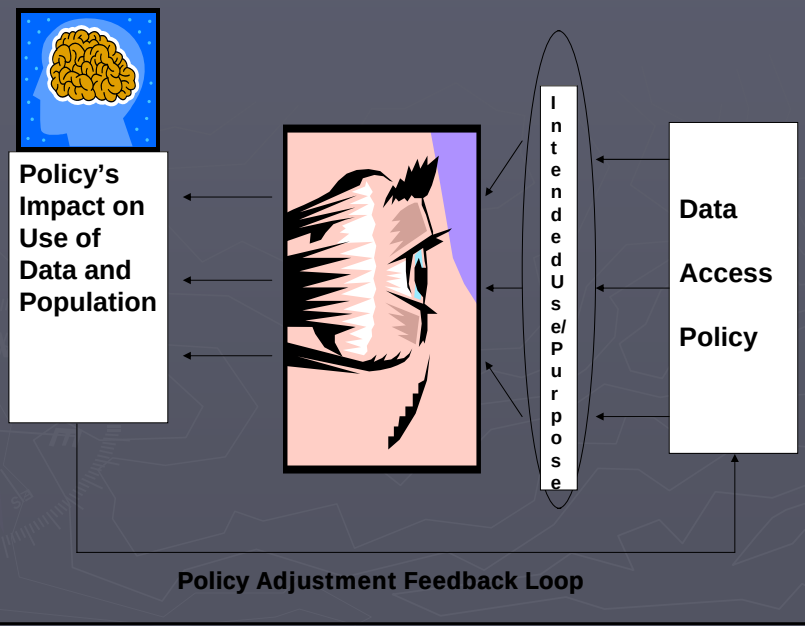
Data Access Pitfalls

1. Needed data may not exist
2. Data may exist, but is held by another sector who can't (or won't) share (personnel issues, funding, mandate, data hoarding)
3. Data exists, but there are barriers to access due to: format; boundary; legislation or gaps in legislation; conservative advice; lack of specific policy for agency access vs academic access; prohibitive charges;

The Data Access Paradox !



Viewing Data Access Policies through the Intended Use Lens



Potential Pathways as we Navigate the Privacy Landscape

- 1. Education of data trustees about proper interpretation of existing legislation and how it fits together
  - Damage can be done by both improper sharing, and improper withholding of information
  - Often, lack of clarity on the interpretation and application of the various pieces of privacy legislation leads bureaucrats to give a default answer of “No” to data sharing requests as the safest practise
  - Certain Public Health legislation may need to be clarified and strengthened in light of new privacy legislation to maintain the ability to safeguard the public’s health

Potential Pathways as we Navigate the Privacy Landscape

- 2. Data Sharing agreements between agencies, or the creation of an intersectoral system when necessary
  - Specify the type and level of sharing allowed under legislation, and that both parties agree to abide by relevant legislation
  - Become more explicit and specific in our mutual data sharing needs and requirements
  - Beware over-compensating tendencies that may unduly restrict future unforeseen data sharing needs (legislation that contains too many lists of circumstances in which data sharing is permissible may be interpreted as excluding all other potential circumstances. Public Health may require some residual general wording about data sharing needs due to emerging public health issues)

Potential Pathways as we Navigate the Privacy Landscape

- 3. Engage the public
  - most probably think/expect RHA's and their providers have access already!
  - Perhaps we should let the public know how their data is not being linked and shared and how that is affecting their care, increasing waste and duplication, compromising safety, and how many times their tax dollars pay to access the same data!
  - ~90% agree to let Stats Can share and link their data for research. How much higher would the support be for sharing with health providers and decision makers who directly impact on their care, and protect them from the spread of infectious disease?

Requirements for the Transfer of Health Information Under New International Law

Dr. Kumanan Wilson, Canada Research Chair, Public Health Policy, University of Ottawa

Bio:

Dr. Kumanan Wilson is a specialist in General Internal Medicine at the Ottawa Hospital. He is also an Associate Professor in the Department of Medicine at the University of Ottawa and a scientist at the Ottawa Health Research Institute. He holds the Canada Research Chair in public health policy.

Dr Wilson's research has focused on studying policy making in areas of health protection and public health security. His work has included analyses of Canadian blood policy and pediatric immunization policy. Dr. Wilson has also conducted research into the impact of intergovernmental relations on public health policy.

Dr. Wilson received his MD from the University of Western Ontario and completed his fellowship training in general internal medicine at McMaster University. He received his MSc. in Health Research Methods from McMaster University.

Requirements for the transfer of health information under new International law

Objectives

1. To describe new requirements for the transfer of health information under the IHR(2005)
2. To describe why such requirements are necessary
3. To illustrate challenges Canada faces in complying with the new requirements

International Health Regulations

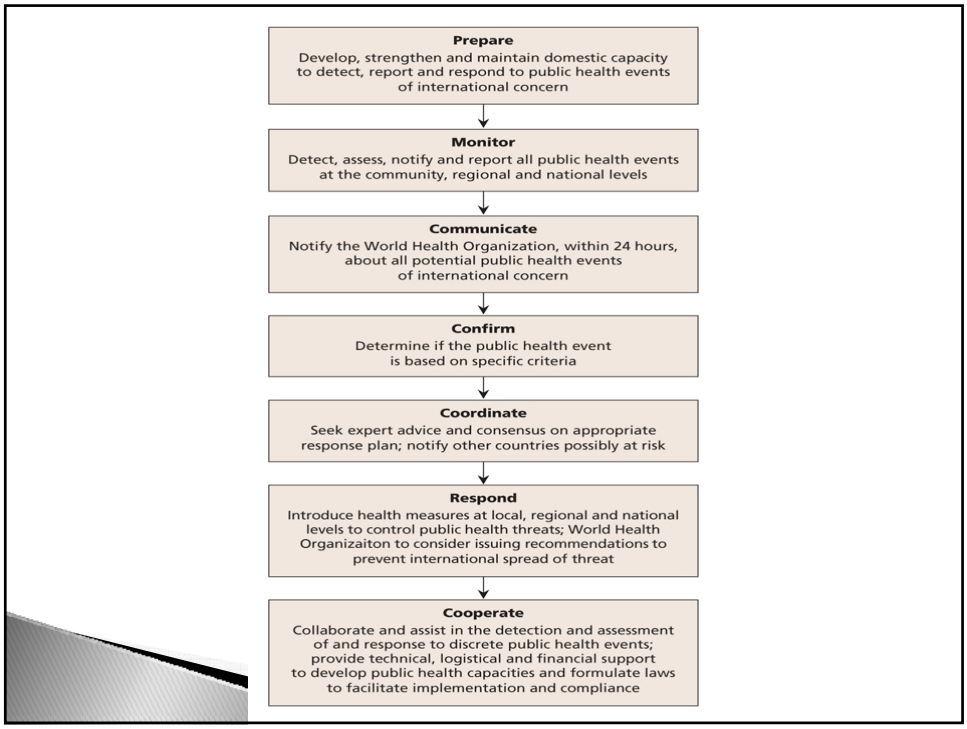
- Approved in May 2005
- The most important document governing the international response to pandemics

The heart of the problem

Table 1. Characteristics of simulated pandemic influenza in the U.S. in the absence of interventions

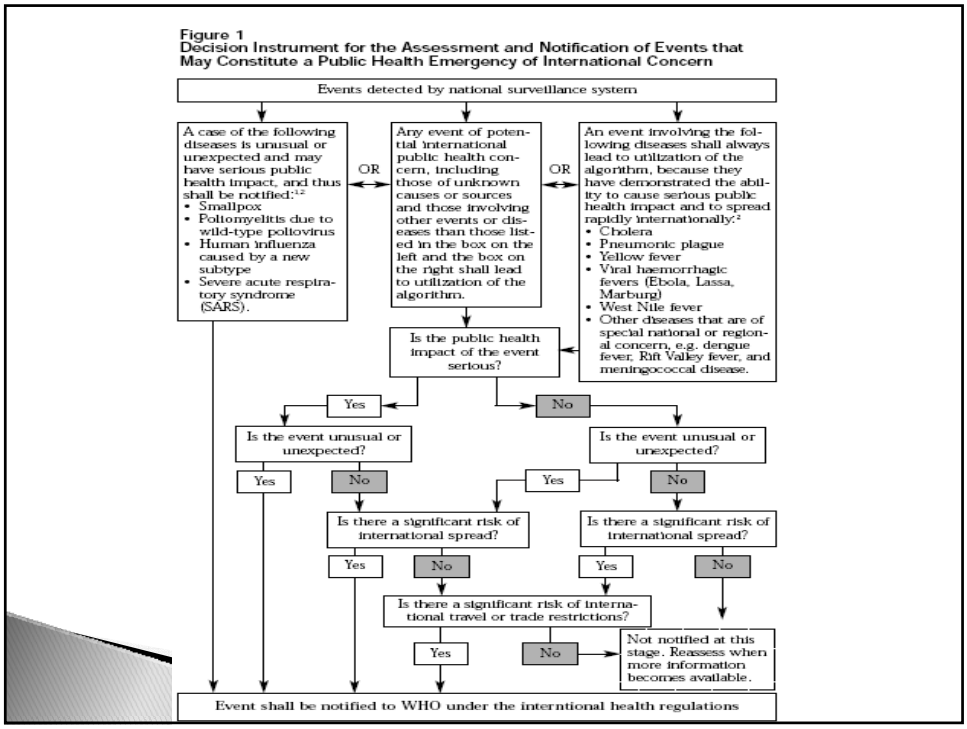
Basic reproductive number, R_0	1.6	1.9	2.1	2.4
Rate of spread: 1,000th ill person*	14	13	12	11
10,000th ill person*	29	24	22	19
100,000th ill person*	48	37	34	29
1,000,000th ill person*	70	52	46	39
Peak of epidemic*	117	85	75	64
Daily number of new cases at peak activity	2.3 M	4.5 M	6.0 M	7.9 M
Number of days with >100,000 new cases	86	68	60	52
Cumulative number of ill persons	92 M	122 M	136 M	151 M

M, million.
*Days after initial introduction.



Assessment

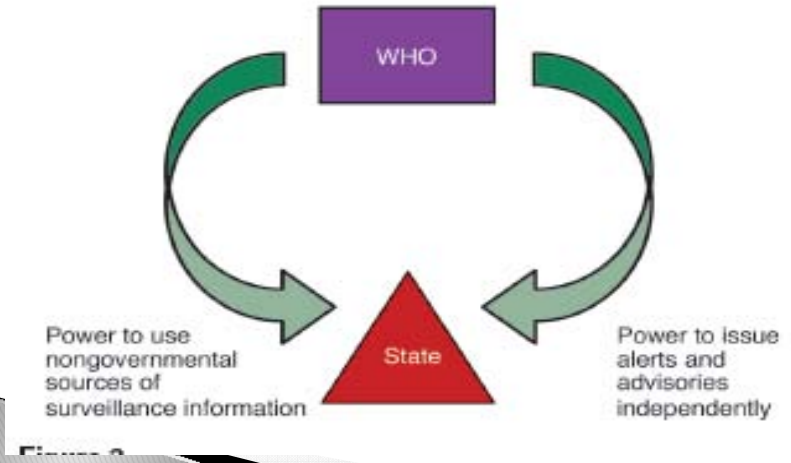
- Member states are required, within 48 hours, to assess any event occurring within their territory and to determine whether it may be a public health emergency using an algorithm



Reporting

- Member states must report potential public health emergencies to WHO within 24 hours after they have identified and assessed them.

WHO double pincer strategy (D. Fidler)



Ongoing communication

- a State Party shall continue to communicate to WHO timely, accurate and sufficiently detailed public health information available to it on the notified event
- case definitions, laboratory results, source and type of the risk, number of cases and deaths, conditions affecting the spread of the disease

Privacy Protection

- Health information collected or received by a State Party pursuant to these Regulations from another State Party or from WHO which refers to an identified or identifiable person shall be kept confidential and processed anonymously as required by national law.

However,

- States Parties may disclose and process personal data where essential for the purposes of assessing and managing a public health risk,

- but State Parties, in accordance with national law, and WHO must ensure that the personal data are:

  (a) processed fairly and lawfully, and not further processed in a way incompatible with that purpose;

  (b) adequate, relevant and not excessive in relation to that purpose;

  (c) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified; and

  (d) not kept longer than necessary.

- Upon request, WHO shall as far as practicable provide an individual with his or her personal data in an intelligible form, without undue delay or expense and, when necessary, allow for correction.

Canada's ability to meet reporting requirements

SARS

- March 2003, SARS comes to Toronto
  - Surveillance systems and communication inadequate

SARS Travel Advisory

- On April 23, the World Health Organization advised international travelers against all non-essential travel to Toronto.
- WHO SARS travel advisory negatively affected economy of Canada
  - ? 1 billion dollar economic impact on Toronto
  - Questionable scientific basis to the advisory

Why did we receive the travel advisory?

- "I don't think we ever really felt that we were working in true partnership with the province"
- "And that inevitably led to a sense of confusion in the outside world, WHO and other countries, as to how far we had this under control." – Federal official

WHO Criticism

- "SARS has shown us that relationships between federal, or central, and provincial or state governments are very important in public health, and very difficult to establish".
- "We understand that this has been a problem in China. It certainly has been a problem in Canada, where there have been difficulties between Health Canada and the provincial government".

- Dr. David Heymann, WHO

Problems Identified by SARS

- Data of "national concern" must be made available to the federal government and other regions
- At present only one region has signed MOU to share data (Ontario)
- Harmonization of data collection to allow sharing between regions
- Requires development of coordinated health surveillance infostructures

Reporting Requirements | **Surveillance Capacity**

Summary

- IHR(2005) requires transfer of data from national to supranational levels
- No guarantee of transfer of information from provincial to national level
- Could put Canada at risk of not meeting international requirements
- Could threaten national and international health security

Privacy and Public Health: A Question of Balance

A Federal Perspective

Gregory W. Taylor, BSc, MD, CCFP, FRCPC, Director General, Office of Public Health Practice, Public Health Agency of Canada

Bio:

Dr. Taylor obtained his MD from Dalhousie University in Halifax where he also completed a family medicine residency. After several years in active primary care in Ontario, he completed a fellowship in Community Medicine at the University of Ottawa and joined Health Canada's Laboratory Centre for Disease Control. Although his initial responsibilities focussed on cardiovascular disease, he has been involved with a wide range of Federal chronic disease activities before joining the Office of Public Health Practice.

He maintains his connection with the University of Ottawa as adjunct professor of Epidemiology and Community Medicine.

Biographie :

Le D^{r} Gregory Taylor est directeur général du Bureau de la pratique en santé publique, Agence de la santé publique du Canada.

Le D^{r} Taylor a obtenu son doctorat en médecine à l'Université Dalhousie, à Halifax, où il a aussi effectué une résidence en médecine familiale. Après de nombreuses années de pratique dans le domaine des soins primaires actifs en Ontario, il a terminé une bourse en médecine communautaire de l'Université d'Ottawa et s'est joint à l'équipe du Laboratoire de lutte contre la maladie de Santé Canada. Ses responsabilités initiales étaient principalement axées sur les maladies cardiovasculaires, mais il a aussi participé à une vaste gamme d'activités de Santé Canada portant sur les maladies chroniques avant de joindre les rangs du Bureau de la pratique en santé publique.

Il conserve encore des liens avec l'Université d'Ottawa à titre de professeur associé en médecine épidémiologique et communautaire.

PUBLIC HEALTH AGENCY *of* CANADA
AGENCE DE LA SANTÉ PUBLIQUE *du* CANADA

Public Health Agency of Canada | Agence de la santé publique du Canada

Canada

A1

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

Privacy ~~vs~~ and Public Health: a question of balance

A Federal Perspective

Dr. Gregory Taylor

Public Health Agency of Canada • santé publique du Canada

Public Health Functions

- Population Health Assessment
- Health Surveillance
- Health Promotion
- Disease and Injury Prevention
- Health Protection
- Public Health Emergency Preparedness and Response

Public Health Agency of Canada -- Strategic Plan: 2007-2012

Surveillance

n. Close observation, especially of a suspected spy or criminal

ORIGIN C**19**: from Fr., from *sur-* 'over' + *veiller* 'watch'

Source: *The Concise Oxford Dictionary*. Ed. Pearsall J. Oxford University Press, 2001.

Surveillance (health)

The tracking and forecasting of any health event or health determinant through the continuous collection of high-quality data, the integration, analysis and interpretation of those data into surveillance products (such as reports, advisories, warnings) and the dissemination of those surveillance products to those who need to know.

National Advisory Committee on SARS and Public Health: Renewal of Public Health in Canada (2003) p. 92.

Surveillance / Research

Surveillance

- Applies existing knowledge to guide health authorities in the use of known control measures
- Directly relevant to monitoring and control needs

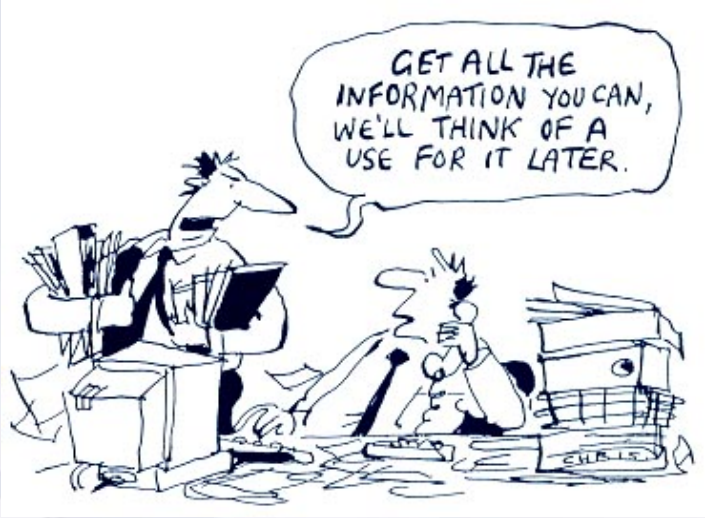
Research

- Pursues new knowledge from which better control measures will result
- Systematic investigation, testing and evaluation, designed to develop or contribute to knowledge

The balancing paradox

Canadians expect to be guarded against unauthorized intrusion into our private lives.

Canadians expect the state to protect populations and our national security.



Individual Rights and Public Health

Disclosure of personal information

- 8. (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

…..(m) for any purpose where, in the opinion of the head of the institution,

- **(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure**, or
- (ii) disclosure would clearly benefit the individual to whom the information relates.

Federal Privacy Act 1980-81-82-83, c. 111, Sch. II "7".

Individual Rights and Public Health

- **Vaccinations**
- **Quarantine**
- **Reportable disease notifications**
- **TB contact tracing / follow up**
- **International Health Regs**
- **Taxation (tobacco, alcohol…)**
- **Disease surveillance**

New Challenges

- the proliferation of information technology,
- information systems and comprehensive databases,
- digitization of health records,
- ability to transfer, link and **re-identify** personal health information, and
- increased demand to protect populations.

Gregory Taylor, BSc, MD, CCFP, FRCP(C)
Director General / Directeur général
Office of Public Health Practice / Bureau de la pratique en santé publique
Public Health Agency of Canada / Agence de la santé publique du Canada

Privacy & Public Health: Ensuring Public Trust

Philippa Lawson, Executive Director, CIPPIC, University of Ottawa

Bio:

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

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

Privacy & Public Health:
Ensuring Public Trust

Electronic Health Information Privacy Conference
Ottawa, ON
03 November 2008

Philippa Lawson
Director, Canadian Internet Policy & Public Interest Clinic
University of Ottawa, Faculty of Law
www.cippic.ca

Definition of Privacy

"the ability to determine for ourselves when, how, and to what extent information about us is communicated to others"

- Alan Weston, 1967

Why Privacy?

- essential to human dignity and autonomy
- key component of free speech and democracy
- underpins relations of mutual trust & confidence, healthy social fabric

The Importance of Trust

- Patient willingness to confide, without fear that personal information will be:
  - used to discriminate re: insurance, employment, credit, government services
  - accessed by others, causing embarrassment or social stigmatization
  - accessed by one who poses a threat
  - used in a manner that is not for the health benefit of the patient (e.g., commercial use)
- Harris surveys show high levels of concern about medical privacy; some people avoid care due to data sharing concerns

The Right to Privacy

- *Nuremberg Code* (1947):
  - " the voluntary consent of the human subject is absolutely essential"
- *Universal Declaration of Human Rights* (1948):
  - "everyone has the right freely to participate in ….scientific advancement and its benefits" (Art.27)
  - "no one shall be subjected to arbitrary interference with his privacy…." (Art.12)

- *European Convention on Human Rights* (1950):
  - "everyone has the right to respect for his private and family life…there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and <u>is necessary</u> in a democratic society…….for the protection of health…." (Art.8)

- *International Covenant on Civil and Political Rights* (1966):
  - "no one shall be subjected to arbitrary or unlawful interference with his privacy…" (Art.17)
  - "no one shall be subjected without his free consent to medical or scientific experimentation" (Art.7)

- World Medical Association, *Helsinki Declaration* (1964, as amended):
  - "the right of the subject to safeguard his integrity must always be respected. Every precaution should be taken to respect the privacy of the subject…" (1975)
  - "It is the duty of the physician in medical research to protect the life, health and privacy and dignity of human subjects" (2000)

- World Medical Association, *Statement on the Use of Computers in Medicine:*
  - "it is not a breach of confidentiality to release or transfer confidential health care information required for the purpose of conducting scientific research…provided the information released does not identify, directly or indirectly, any individual patient in any report of such research….or otherwise disclose patient identities in any manner…" (1973, amend.1983)

- Council of Europe, Recommendation on the Use of Medical Data (1997):
  - Scientific Research (s.12)
    - Whenever possible, use anonymous data
    - Where impossible (+ legit purposes),must have:
      - "free, express, informed consent" of data subject; or
      - defined project, important public interest, authorization of legally designated body, impractical to get consent, and data subject doesn't object; or
      - the research "is provided for by law and constitutes a necessary measure for public health reasons"

SCC – health data privacy

- Supreme Court of Canada, *McInerney v. MacDonald* (1992):
  - "Information about oneself revealed to a doctor acting in a professional capacity remains, in a fundamental sense, one's own….is held in a fashion somewhat akin to a trust….gives rise to an expectation that the patient's interest in and control of the information will continue."

Cdn AIDS Society v. Ontario

- Mandatory release of tainted blood records to public health authorities (1995)
  - CAS challenged as breach of privacy under ss,7 and 8 of *Charter*
- Ont. Court ruled violation was justified given:
  - severity of public health risk
  - mandatory release of data = rational approach
  - no other workable, less intrusive option
  - public health risk more serious than individual privacy violations

Health Info Research rules

- Consent if possible
- De-identification if possible
- Special body (eg: REB) must approve, s.t.:
  - Anonymous data won't suffice
  - Impractical to get consent (if none)
  - Adequate safeguards to protect confidentiality
  - No disclosure of personal data
  - Public importance of research outweighs individual privacy

Health Research

- rarely serves the interest of the research subject directly
- often associated with third party (commercial) interests
- often driven by prospect of financial gain
- researchers often dependent on funding from private entities
- high stakes; heavy competition
- success measured in terms of number of publications or patents – not contribution to public health

Concerns

- Assumes properly constituted, well-functioning REBs
  - Resources of REBs?
  - Transparency, accountability, oversight?
- Assumes responsible, careful HICs
- Undue influence of pharmaceuticals/biotech industry
- Paternalistic approach (vs. individual consent)
  - Should individuals be forced to participate in research for benefit of future generations?

One expert view

- "No one has a duty to participate in medical research on behalf of the health of future patients and generations."
- "Participation in medical research – through personal medical data…- is a gesture of altruism comparable to the donation of human biological material for other patients' health care."
  - Dr. Henriette Roscam Abbing, Univ. of Utrecht

Why is health privacy important?

- Particularly sensitive information
  - subject to prejudice; labelling; redlining
  - consequences for:
    - social status; human relations
    - employment opportunities
    - insurance
    - government services
    - marketplace options
    - identity theft/fraud

Reframing the Problem

- Clash of values:

  collective/public health vs. individual privacy?

  OR

- Full accounting of social costs and benefits of both public health and privacy?

www.cippic.ca

Session 2A: Privacy in Practice

Session Chair: Michael Power, eHealth Ontario

Bio of Chair:

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.

Do Data Breach Disclosure Laws Reduce Identity Theft?

Sasha Romanosky, Heinz School of Public Policy and Management, Carnegie Mellon University

Abstract:

Identity theft resulted in corporate and consumer losses of $56 billion dollars in 2005, with about 30% of known identity thefts caused by corporate data breaches. Many US states have responded by adopting data breach disclosure laws that require firms to notify consumers if their personal information has been lost or stolen. While the laws are expected to reduce identity theft, their full effects have yet to be empirically measured.

Romanosky will present the results of his study, which aims to fill this knowledge gap by providing a measure of the effectiveness of breach disclosure laws in the US. A panel from the US Federal Trade Commission was used to determine the impact of data breach disclosure laws on identity theft over the years 2002 to 2007.

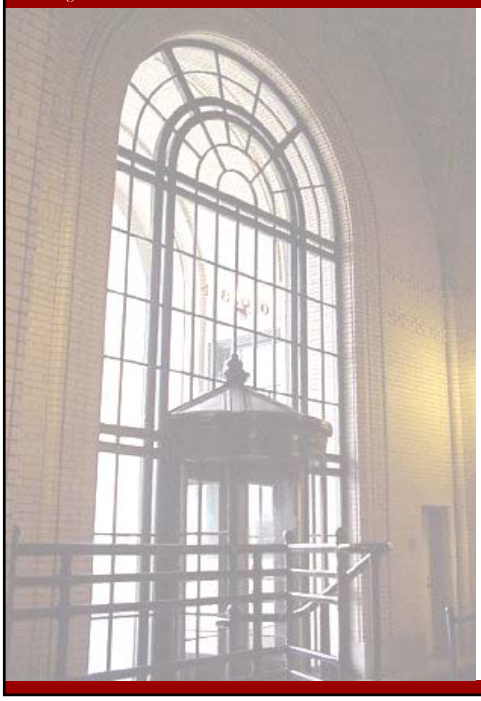
Adoption of data breach disclosure laws were found to reduce the rate of identity thefts by just under 2%, on average. While this effect is marginal, reducing identity theft is only one means by which these laws can be evaluated: we appreciate that they may have other benefits such as reducing the average victim’s losses or improving a firm’s security and operational practices.

Bio:

Sasha Romanosky, CISSP, holds a Bachelor of Science degree in Electrical Engineering from the University of Calgary. He has been working with internet and security technologies for over 10 years, predominantly within the financial and e-commerce industries at companies such as Telus, Morgan Stanley and eBay. He is coauthor of "J2EE Design Patterns Applied" and "Security Patterns: Integrating Security and Systems Engineering" and has published other works on information security.

He developed the FoxTor tool for anonymous web browsing and is co-developer of the Common Vulnerability Scoring System (CVSS), an open framework for scoring computer vulnerabilities. Sasha is currently a PhD student at the Heinz School of Public Policy and Management at Carnegie Mellon University. His research field is the economics of information security.

Carnegie Mellon



Do Data Breach Disclosure Laws Reduce Identity Theft?

Sasha Romanosky
Rahul Telang
Alessandro Acquisti

Ottawa, Canada
November 2008

Carnegie Mellon Heinz School

Carnegie Mellon

The problem: Identity theft

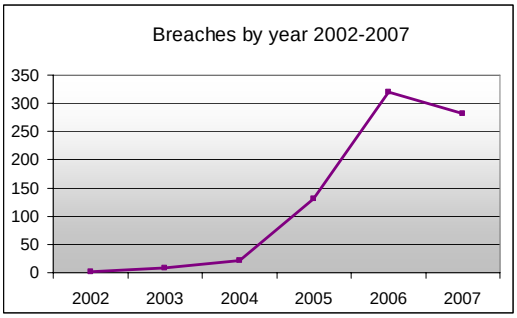
- FTC recorded over 250,000 idtheft consumer complaints (2007)
- Actual number of victims estimated to be around 8.1 M
- Total amount stolen is estimated at over $45B (Javelin, 2008)
- Impact includes costs to:

  Consumers: time repairing credit, lawyer fees, lost wages, etc

  Firms: lost revenue, civil law suits, govt fines, consumer redress
  - Choicepoint (162k records): $10m FCRA fine + $10m civil lawsuit + $6m other = $26m
  - TJ MAX (~95m records): $160m

Carnegie Mellon Heinz School

The cause? Data breaches



About 800 known breaches between 2000-2007 (attrition.org)
~ 70% caused by hackers (stolen data)
~ 75% include SSN
~ 32% from businesses, 32% educational, 26% govt, 10% medical

The solution? Data breach disclosure laws

- Data breach disclosure laws require firms to notify consumers when their personal information is lost or stolen
- Many feel these laws will reduce idtheft
  - 4 US Congressional hearings in 2005
  - Many laws are titled, “identity theft prevention”
  - “among the most important advances that the [UK] could make in promoting personal internet security” (Science and Tech Committee, 2007)
- Significant precedent of disclosure (transparency) laws in the US: EPCRA, FDA, Nutrition labeling, Fuel Octane levels, FOIA

But why should they work?

Sunlight as a disinfectant (Justice Brandeis, 1933)

- Highlighting a firm's poor security practices will encourage firms to improve (reducing the externality)
- "Drive performance through transparency and public oversight" (Mulligan, 2007)

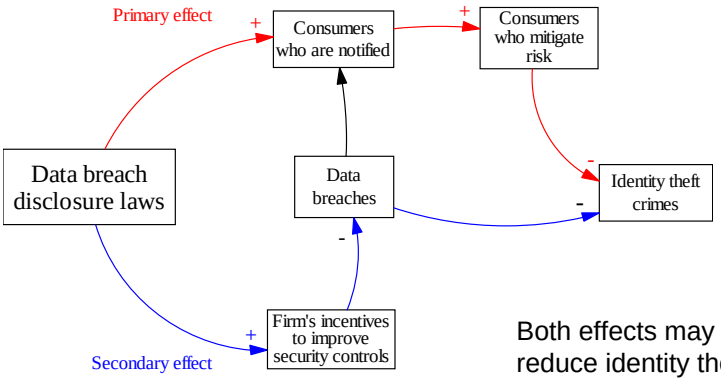
Right to know (Magat & Viscusi, 1992; Solove, 2004)

- Consumers have the right to know when a firm is using, or *abusing* their information.
- By notifying consumers of breaches, they can mitigate the risks (close accounts, warn banks/CC firms, freeze credit, idtheft insurance)

…but not everyone agrees

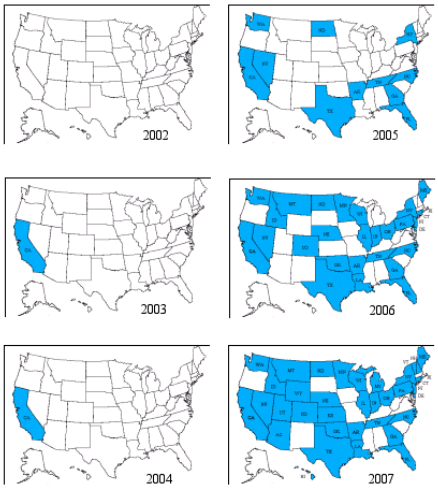
- Laws cause firms and consumers to incur unnecessary costs, leading to an overall worse outcome, esp. if the probability of idtheft from a breach is < 2% (idAnalytics, 2006; Ponemon, 2008)
- The externality is not nearly so grave: firms already bear ~90% of the cost of breaches (Javelin Research, 2003, 2005, 2006)
- Consumers could become desensitized to numerous breach notifications, ignoring all of them (GAO, 2007)
- Stifles ecommerce and R&D by discouraging firms to innovate (Rubin and Lenard, 2005)

Data Generating Process



Both effects may reduce identity theft

Adoption of state laws, 2002 - 2007

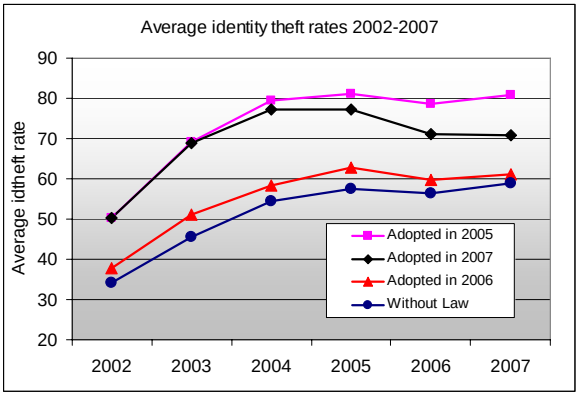


Year	# adopters
2002	0
2003	1 (+1)
2004	1
2005	11 (+10)
2006	28 (+17)
2007	38 (+10)

Identity theft data

- The FTC maintains a national database of consumer-reported identity theft complaints (1-877-ID-THEFT,www.ftc.gov)
- Uniform collection and management of data between states
- Mined by law enforcement to catch offenders
- Examples of idtheft (FTC, 2006):
  - Credit card charges (new, existing account, ~25%)
  - Loan, bank fraud (mortgage, car, etc, ~21%)
  - Phone and Utilities (unauthorized charges, new accounts, ~16%)
  - Government, medical benefits, etc (~10%)

Idtheft for states with / without law



Idtheft for states *with* and *without* law appear to follow same trend.

Idtheft rate: number of crimes per 100,000 people

Data Collection

- We acquired monthly data for 2002-2007, from FTC using Freedom Of Information Act
- Aggregated to semi-annual periods (smallest period over which we expect to see an effect of law)
- 12 periods * 50 states (+ D.C.) = 612 obs
- Reported data: frequently used (Blumstein et al, 1991) and represents the best we have on identity theft

Econometric Model

- $idtheft_{st} = \beta_0 + \beta_1 hasLaw_{st} + \beta_2 breaches_{st} + \sum \rho_{st} Related_{st} + \sum \delta_{st} Economic_{st} + \sum \alpha_{st} Crime_{st} + \theta_s + \lambda_t + \varepsilon_{st}$
- A familiar approach to analyzing such policy issues
- Identification comes from variation across *state and time*
- $Related_{st}$: credit freeze laws, FACTA, data breaches
- $Economic_{st}$: population, state GDP, income, unemployment
- $Crime_{st}$: fraud, murder, robbery, burglary, motor-vehicle theft
- $cor(\varepsilon_{s,t}, \varepsilon_{s,t+1}) \neq 0$, SE are cluster-corrected by state

Results

Dep Var: idtheft rate	(1) Basic	(2) Lagged Law	(3) Weighted
Has Law	-1.28*		-0.73**
	(0.70)		(0.35)
6 months old		-0.03	
		(0.67)	
12 months old		-1.09	
		(0.85)	
18 months old		-0.43	
		(0.98)	
R-squared	0.79	0.79	0.66

N=612, all regressions run with state cluster-corrected SE

Standard errors In parentheses, *** significant at 1% level, **5%, *10%

Results in context

- To place in context, for 2005, this corresponds to:
  - ~2% reduction in idtheft rate, or
  - $1 billion savings to firms and consumers

Research	Treatment	Outcome measure (Result)
Donohue (2004)	Right-to-Carry laws	Violent crime rate: -3% to +4% Murder rate: -8% to +3% MV theft rate: -7% to +15% Property crime rate: 0% to +10%
Epple and Visscher (1984)	Coast guard monitoring	Oil spill frequency: +2.1% Oil spill volume: - 3.1%
Cohen (1987)	Coast guard monitoring	Oil spill frequency: -2% Oil spill volume: -1.7%
Hamilton (1995)	Disclosure of toxic release (TRI)	Stock price: -0.3%
Acquisti, Telang, Friedman (2006)	Disclosure of security breach	Stock price: -0.6%

Policy Recommendations

- Most people claim to be concerned about identity theft, yet they don't respond to breach notifications (Ponemon, 2008)
- Why the disconnect? Consumer decision errors: optimism bias, rational ignorance, status quo bias
- R1: Craft consistent notifications that provide actionable information to consumers
- R2: Establish an authoritative source for all breaches (useful to consumers, researchers, policy makers)

Conclusions

- We reveal only a marginal effect. A lack of stronger influence may be due to the following:
  - Our regression analysis may be too blunt an instrument with which to measure it
  - The reported data may be a poor source, but it's the best we have
- Effectiveness of the law is maximized when both firms and consumers take appropriate actions
- There may be other benefits of the laws
  - Early notification reduces consumer loss (FTC 2007, Javelin 2007)
  - Improves firm practices (Choicepoint; Hannaford, VA)

Questions?

http://explodingdog.com/rocketguy.gif

Privacy Versus the Right to Know

David McKie, Investigative Reporter, CBC News

Abstract:

David McKie will discuss some of the investigative techniques that are often used, focusing on the challenges investigative reporters face when attempting to use the Access to Information Act to obtain records needed for investigations into areas such as drug, food and air safety. Even with the new provision in the Act which imposes a duty to assist onto the shoulders of ATIP officials, there remains some difficulty with the use of privacy concerns to withhold key information that allows reporters to, among other things, pin-point areas of the country where certain adverse drug reactions may be a problem. Privacy concerns also staunch the flow of crucial information between the provincial and federal governments, for example, in areas such as infectious diseases. Such a lack of information makes it extremely difficult for investigators to do their jobs.

Bio:

David McKie is an award-winning, Ottawa-based journalist with the Investigative Unit for CBC News. He specializes in public policy areas such as drug, food and air safety. He uses the federal Access to Information law, provincial freedom-of-information laws, and computer-assisted reporting techniques. David teaches investigative research techniques at Carleton University's School of Journalism and edits the Canadian Association of Journalists' Media magazine. He hosts a web site that tracks access-to-information requests. And, finally, he is co-author of two journalism textbooks on investigative techniques.

PRIVACY VERSUS THE RIGHT TO KNOW

Two concepts that are at odds at a time when the philosophies that define both concepts are pulling in opposite directions

Privacy versus the right to know

- The pressures to maintain privacy are many
- The deregulation in industrial sectors such as the food, drug and transportation
- Information such as audits are now deemed to be the property of the private sector
- There is continued conflict between the federal government and the provinces when attempting to share health information such as infectious diseases

Privacy versus the right to know

- The Harper government has shut down the CAIRS site, which gave users across the country the ability to piggy-back on access requests
- There has been no meaningful reform of the federal act since it became law, and many access advocates say that serious reform is long overdue

Privacy versus the right to know

- Federal access to information coordinators now have a "duty to assist", which could enhance our right to know
- But the duty to assist is mitigated by factors such as short-staffed ATI offices; a heavy-handed PCO and PMO
- And the continued reluctance of users such as journalists to get the most out of access to information

Privacy versus the right to know

- The system has been described as "paralyzed"
- Backlogs for requests are a fact of life
- The Information Commissioner's Office is mired in a quagmire
- Court decisions such as the CBC's failed attempted to obtain more information from Health Canada's adverse drug reaction database can be seen as a setback

Privacy versus the right to know

- There is much at stake, as the forces controlling privacy and access pull in opposite directions
- History has demonstrated that major stories on adverse drug reactions, political conflict of interest, profligate spending and the treatment of Afghan detainees would not have been possible without the use of the access law
- How much more remains hidden that needs to be uncovered

Privacy versus the right to know

- There is a challenge for journalists
- Know the laws at the federal and provincial level
- Do your homework before embarking on request
- Be more strategic
- Be vigilant
- Push to obtain information informally where possible, and don't take no for an answer

Decision support and the safe use of health data for secondary purposes

Elaine Sawatsky, Privacy Consultant

And Ognjenka Djurdjev, Corporate Director Decision Support, Provincial Health Services Authority, British Columbia

Bio:

Ms. Elaine Sawatsky is a privacy professional with extensive and up-to-date knowledge of Canada's national and provincial health environment and experience with Provincial Health Ministries, physicians and other healthcare providers, specializing in Privacy and Security strategies, policies and programs. She has an in-depth understanding of Security and Privacy programs and practices. Her focus includes a privacy strategy for First Nations, provincial EHR programs, secondary use, data warehousing including issues related to strategic solutions, governance, policy, anonymization and service design. Elaine is an independent consultant.

Privacy in Practice
Oct. 2008

E. Sawatsky & Assoc. .Inc

Conflicting Goals?

- *We want our society to provide good healthcare & provide human rights, respect and a society that values us*
- Privacy advocates are concerned

E. Sawatsky & Assoc. .Inc

Good Health Care

- Clinical care
  - EHR – “primary purposes”
- Management of care delivery
  - Transformed and linked data – “secondary purposes”
- Individual vs. societal perspective
  - Direct and indirect benefit

E. Sawatsky & Assoc. .Inc

The World is Changing

- The world and its complexity
- The technology
- Persons and their expectations
- All of which relate to both privacy and the EHR as well as how we use health data for other purposes

E. Sawatsky & Assoc. .Inc

Complex Environments

There is greater risk due to:

- More stakeholders
- Political issues
- External partners (i.e. less control)
- New technology
- Less flexible organizational culture
- High investment
- Low tolerance for failure

Complex Environments

But most of all the complexity comes from ….

the need to integrate data, to provide integrated Services …….

…..to an *'integrated' Individual*

A integrated 'system' includes: data, technology, people and processes – within a scope (program, dept, organization, the world)

New Approach to Privacy

Requires solutions:

- Greater oversight
- More planning, reporting, communication
- More data protection
- Privacy culture

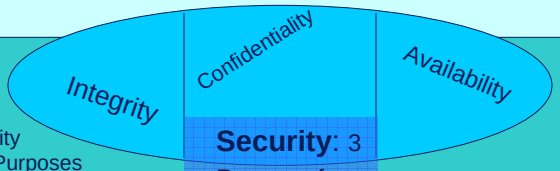
How We Approach Privacy Needs to Change

- Often the previous approach has failed
- Privacy is a societal construct
- We cannot build a new concept with outdated methods
- Privacy as an industry is not yet well evolved (what is a PIA for anyway?)
  - A task on a project plan?
  - An exam at the end of your project?
  - A risk management exercise?

Privacy & Security

Privacy

Includes other privacy concepts e.g.
Rural living, curtains, hedges, behaviour



Security: 3 Reasons for Safeguards

Privacy:
- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting use, disclosure, retention
- Accuracy
- Openness
- Individual Access
- Challenging compliance

Protection of Information *or* Informational Self-determination

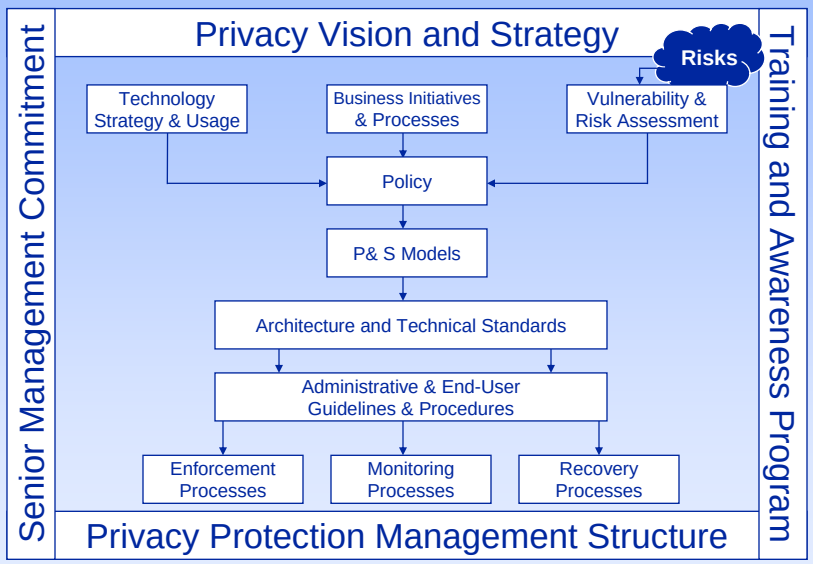
E. Sawatsky & Assoc. .Inc

Addressing Privacy Risks: Define Scope

- Privacy is effected & supported by:
  - Organizational – Org Programs
  - Departmental – lower level policy, education, and behaviours
  - System/Technical – at this point it is no longer privacy at all, but security (confidentiality)

E. Sawatsky & Assoc. .Inc

Privacy Framework



PriceWaterhouseCoopers E. Sawatsky & Assoc. .Inc

Complex Environments

- Requires a strong business focus in order that the various risks are:
- Identified,
- Assessed,
- Mitigated,
- Balanced,
- ……. And privacy risk is only one

- Requires the assumption that data will be protected
- Requires understanding of the 'business' within its broad context: financial, legal, public relations

E. Sawatsky & Assoc. .Inc

Understand Where P/S fits

- Interleaved, integrated
- Privacy is a risk like any other
- Begin addressing it at the beginning
- Differentiate between risk to the project and other risk e.g. privacy
- Mitigating one risk can create more elsewhere
- Understand your business

Privacy Approach

- Privacy need not be a barrier to success
- Privacy Protection is a program, a process, not a project
- PIAs can be many things: useful, or not
- Privacy protection is not about writing PIAs
- A perfectly protected environment results in a perfect PIA
- That only happens when program privacy is designed in isolation

The Provincial Health Services Authority (PHSA)

- Primary role to ensure that B.C. residents have access to a coordinated network of high-quality specialized health care services
- PHSA operates 8 provincial agencies including BC Children's Hospital, BC Transplant, BC Cancer Agency and Riverview Hospital (Mental Health)
- PHSA also responsible for specialized provincial health services like surgical and trauma services

E. Sawatsky & Assoc. .Inc

PHSA Strategic Goals

- Quality and safety of patient care
- Improved outcomes
- Increased efficiency
- Ensure capacity and resources to meet needs
- Education and research
- Financially sustainable

E. Sawatsky & Assoc. .Inc

PHSA Business Intelligence & Data Warehousing Transformation

▪ Quality and safety of patient care →	▪ Linked clinical & operational data, “numerator” and “denominator” from different systems, ongoing monitoring
▪ Improved outcomes →	▪ Longitudinal patient records, “downstream” results
▪ Increased efficiency →	▪ Operational research data, evidence based process re-engineering
▪ Ensure capacity and resources to meet needs →	▪ Projections based on linked registry and population data
▪ Financially sustainable →	▪ Forecasting using integrated financial, operational and clinical data

E. Sawatsky & Assoc. .Inc

PHSA Programs

- Legally compliant
- Good corporate citizen
- Credible
- Trusted
  - When the organization fails in one area it can create a lack of trust so that opportunities are lost in another. E.g. a privacy breach may affect a future business opportunity.

E. Sawatsky & Assoc. .Inc

The PHSA BI & DW Requirements

- Legal standing under FIPPA
- Appropriate governance
- Accountability
- Policy
- Defined Purpose
- Controls
- Default: Anonymisation

Legal Standing

- FIPPA allows for Integrated Programs
- Legal indicia of control
- Governance
- Budgets
- Agreements
- Terms of Reference
- Operating Policy

Governance: Demonstrate Control

- Understand Risks
- Measure Risks
- Reduce or accept, as appropriate
- Risks in Collection, Use & Disclosure
- Risk in retention
- Risks in destruction

Risks: Collection

- Privacy law: collect only what you need
- Data Warehouse = all data
- How do you know tomorrow's questions?
- Are we prepared to take the risk?
- How can it be reduced?
- MBUN? Anonymous?

Risk: Use

- Limit access to identifiable data
- Computer queries don't recognize people
- Computers have no prejudice
- Reliable
- Consistent

Risk: Use

- Default: Anonymisation
  - Consistent and practical method to use linked and anonymized data
  - Strong statistical foundation
  - Peer reviewed algorithms
  - Assessment of risk of re-identification
- Strong operational policy
- Flawless execution
- Policy allows one to say No

Risk: Disclosure

Data represents a person, in a certain way.

It can be:

- Complete, or not
- Accurate, or not
- Relevant, or not
- Unbiased, or not

from a number of perspectives

- Risk of identifying a specific person one knows
- Risk of identifying person as a member of a group
- Data subjects must know absolutely that data is never put at risk

Risk: Disclosure

- For what purposes may data be disclosed?
- What technical controls are applied?
- What administrative controls are applied?
- Expensive? No question
- Valuable? No question

Risk: Retention

- Physical and technical and administrative controls must be absolutely impeccable
- Destruction techniques must be solid
- Openness and transparency for all collection, use and disclosure

Risks: Retention

- Risks to groups – First Nations, PWA, family relationships
- Linkage policy must be carefully set
- Privacy law says: no harm
- Who decides what is harmful?

Changes Required

- Assumptions – we must remind ourselves as we go on:
  - Identified data disclosed only under strict control, very limited and justified
  - No access to identifiable data except in justifies and defined circumstances
  - Continued oversight to ensure procedures don't slip
  - Process to define new purposes
  - OPENNESS
  - TRUST

Contacts

- Elaine.Sawatsky@Telus.net
- Ognjenka.Djurdjev@phsa.ca

Session 1B: Location Privacy

Session Chair: David Buckeridge, MD Ph, McGill University, Department of Epidemiology and Biostatistics and McGill Clinical and Health Informatics

Session Description:

In this session speakers will address the intersection of geographical information and geospatial technologies with privacy. Speakers will offer examples of re-identification of individuals from maps and consider methods for minimizing the likelihood of this type of re-identification occurring.

Bio of Chair:

David Buckeridge, M.D. Ph.D., is an Assistant Professor of Epidemiology and Biostatistics at McGill University in Montreal where he holds a Canada Research Chair in Public Health Informatics. He is also a Medical Consultant to the Institut national de santé publique du Québec and the Direction de santé publique de Montréal. His research focuses on public health informatics and particularly on the informatics of public health surveillance. Current research projects include developing and evaluating systems for automated surveillance in community and hospital settings. He has a M.D. from Queen's University in Canada, a M.Sc. in Epidemiology from the University of Toronto, and a Ph.D. in Biomedical informatics from Stanford University. Dr Buckeridge is also a Fellow of the Royal College of Physicians and Surgeons of Canada with specialty training in Community Medicine.

Christopher Cassa, Ph.D., a graduate of the Harvard-MIT Division of Health Sciences and Technology, is a research fellow at the Children's Hospital Informatics Program at Harvard Medical School in Boston, MA. He has researched a wide range of medical privacy and identifiability issues. Applying quantitative approaches, he has helped developed two anonymization techniques for geographical data and investigated the re-identification potential of geographical data shared in textual and map form. His most recent work has investigated the ability to infer genotypes from family members of research proband, and how readily research datasets can be used to identify family members and familial phenotypes.

Privacy and Identifiability in Clinical Research, Personalized Medicine, and Public Health Surveillance

Christopher Cassa, Ph.D., Research Fellow, Harvard Medical School

Abstract:

Electronic transmission of protected health information has become pervasive in research, clinical, and public health investigations, posing substantial risk to patient privacy. From clinical genetic screenings to publication of data in research studies, these activities have the potential to disclose identity, medical conditions, and hereditary data. To enable an era of personalized medicine, many research studies are attempting to correlate individual clinical outcomes with genomic data, leading to thousands of new investigations. Critical to the success of many of these studies is research participation by individuals who are willing to share their genotypic and clinical data with investigators, necessitating methods and policies that preserve privacy with such disclosures.

We explore quantitative models that allow research participants, patients and investigators to fully understand these complex privacy risks when disclosing medical data. This modeling will improve the informed consent and risk assessment process, for both demographic and medical data, each with distinct domain-specific scenarios. First, the de-identification and anonymization of geospatial datasets containing information about patient home addresses will be examined, using mathematical skewing algorithms as well as a linear programming approach. Next, we consider the re-identification potential of geospatial data, commonly shared in both textual form and in printed maps in journals and public health practice. We also explore methods to quantify the anonymity afforded when using these anonymization techniques. Last, we discuss the disclosure risk for genomic data, investigating both the risk of re-identification for SNPs and mutations, as well as the disclosure impact on family members.

Bio:

Christopher Cassa, Ph.D., a graduate of the Harvard-MIT Division of Health Sciences and Technology, is a research fellow at the Children's Hospital Informatics Program at Harvard Medical School in Boston, MA. He has researched a wide range of medical privacy and identifiability issues. Applying quantitative approaches, he has helped developed two anonymization techniques for geographical data and investigated the re-identification potential of geographical data shared in textual and map form. His most recent work has investigated the ability to infer genotypes from family members of research proband, and how readily research datasets can be used to identify family members and familial phenotypes.

Privacy and Identifiability in Clinical Research, Personalized Medicine, and Public Health Surveillance

Christopher Cassa

Children's Hospital Informatics Program
Harvard-MIT Division of Health Sciences and Technology

Transmission of PHI Pervasive

- The use of protected health information for spatial analysis is pervasive and critical for
  - Exchange of health data, NHIN
  - Disease detection and surveillance
  - Identifying etiology, patterns, correlates, and predictors of disease

Children's Hospital Boston Informatics Program
Harvard-MIT Division of Health Sciences and Technology

Balance between Privacy and Data Use

- Pervasive in research, medicine, and public health investigations, posing risk to privacy
- Disclose identity, medical conditions, and hereditary data

Balance between privacy and research and public health

Collaborators

- The work was supported by R01LM007970-01 and R01-LM009375-01A1 from the National Library of Medicine, National Institutes of Health

Kenneth Mandl MD MPH (CHIP)
John Brownstein PhD (CHIP)
Shannon Wieland PhD (CHIP)
Karen Olson PhD (CHIP)
Marc Overhage MD PhD (Regenstrief)
Shaun Grannis MD MS (Regenstrief)

Topics

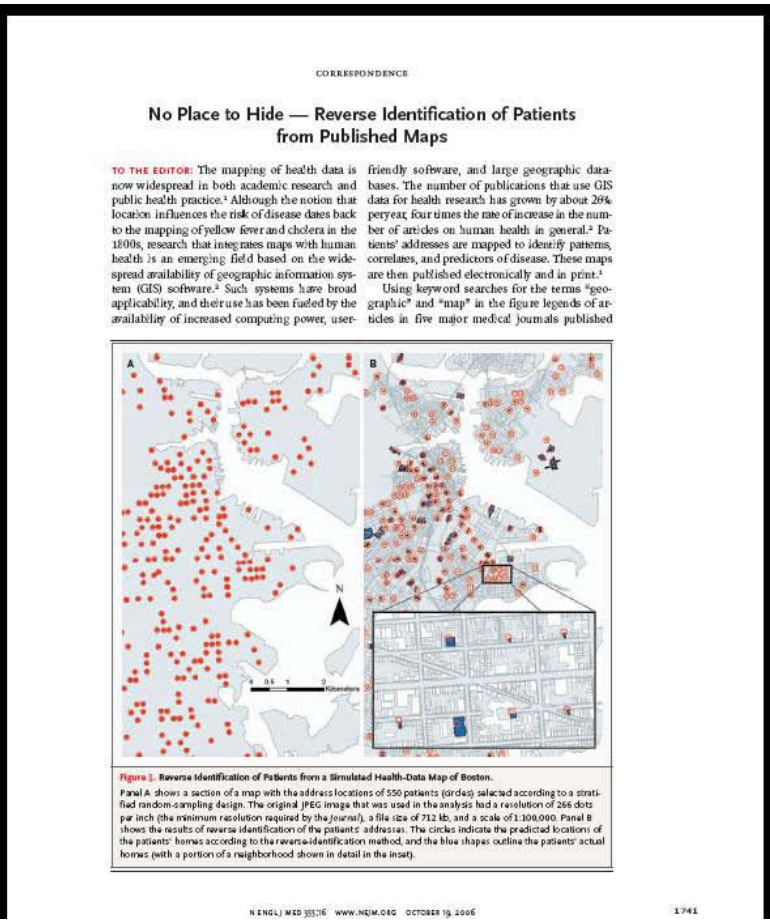
1. Anonymization of geospatial datasets containing patient home addresses
2. Re-identification potential of geospatial data, commonly shared in both textual form and in printed maps
3. Disclosure risks for genomic data and impact on family members

Topics

1. Anonymization of geospatial datasets containing patient home addresses
2. Re-identification potential of geospatial data, commonly shared in both textual form and in printed maps
3. Disclosure risks for genomic data and impact on family members

Revealing Addresses from Published Maps

Brownstein, Cassa, Mandl NEJM Oct. 2006



CORRESPONDENCE

No Place to Hide — Reverse Identification of Patients from Published Maps

TO THE EDITOR: The mapping of health data is now widespread in both academic research and public health practice.[1] Although the notion that location influences the risk of disease dates back to the mapping of yellow fever and cholera in the 1800s, research that integrates maps with human health is an emerging field based on the widespread availability of geographic information system (GIS) software.[2] Such systems have broad applicability, and their use has been fueled by the availability of increased computing power, user-friendly software, and large geographic databases. The number of publications that use GIS data for health research has grown by about 26% per year, four times the rate of increase in the number of articles on human health in general.[2] Patients' addresses are mapped to identify patterns, correlates, and predictors of disease. These maps are then published electronically and in print.[1]

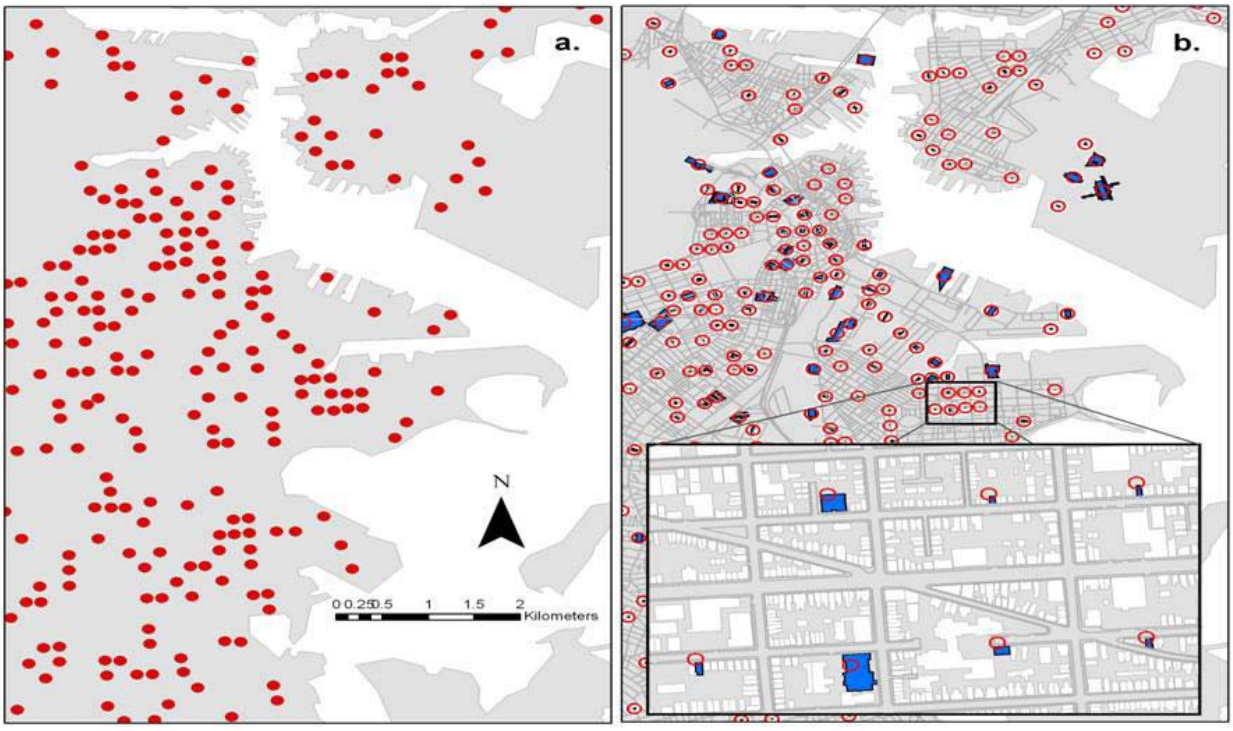
Using keyword searches for the terms "geographic" and "map" in the figure legends of articles in five major medical journals published

Figure 1. Reverse Identification of Patients from a Simulated Health-Data Map of Boston.

Panel A shows a section of a map with the address locations of 550 patients (circles) selected according to a stratified random-sampling design. The original JPEG image that was used in the analysis had a resolution of 266 dots per inch (the minimum resolution required by the *Journal*), a file size of 712 kb, and a scale of 1:100,000. Panel B shows the results of reverse identification of the patients' addresses. The circles indicate the predicted locations of the patients' homes according to the reverse-identification method, and the blue shapes outline the patients' actual homes (with a portion of a neighborhood shown in detail in the inset).

N ENGL J MED 355;16 WWW.NEJM.ORG OCTOBER 19, 2006 1741

Re-identified 79% of points from low resolution map



Background

- The use of protected health information for spatial analysis is common and critical for
  - Exchange of health data in health record networks
  - Disease detection and surveillance systems
  - Identifying etiology, patterns, correlates, and predictors of disease

Key Concept: *k*-Anonymity

- Degree of anonymization is defined in terms of *k*-anonymity – where each patient is not identifiable among *k* other patients.

L. Sweeney. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570.

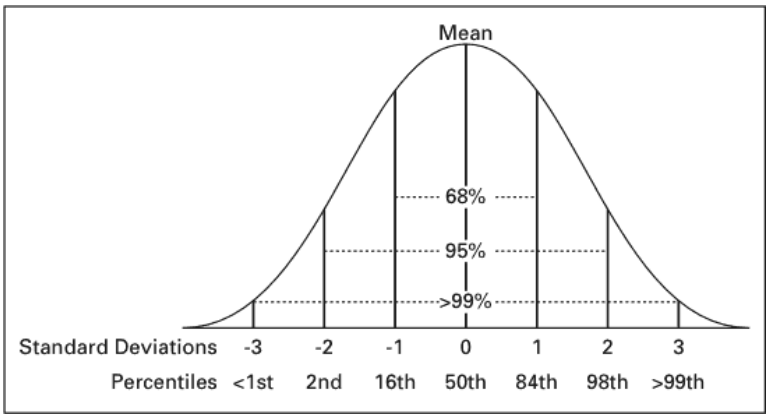
Current Anonymization Methods

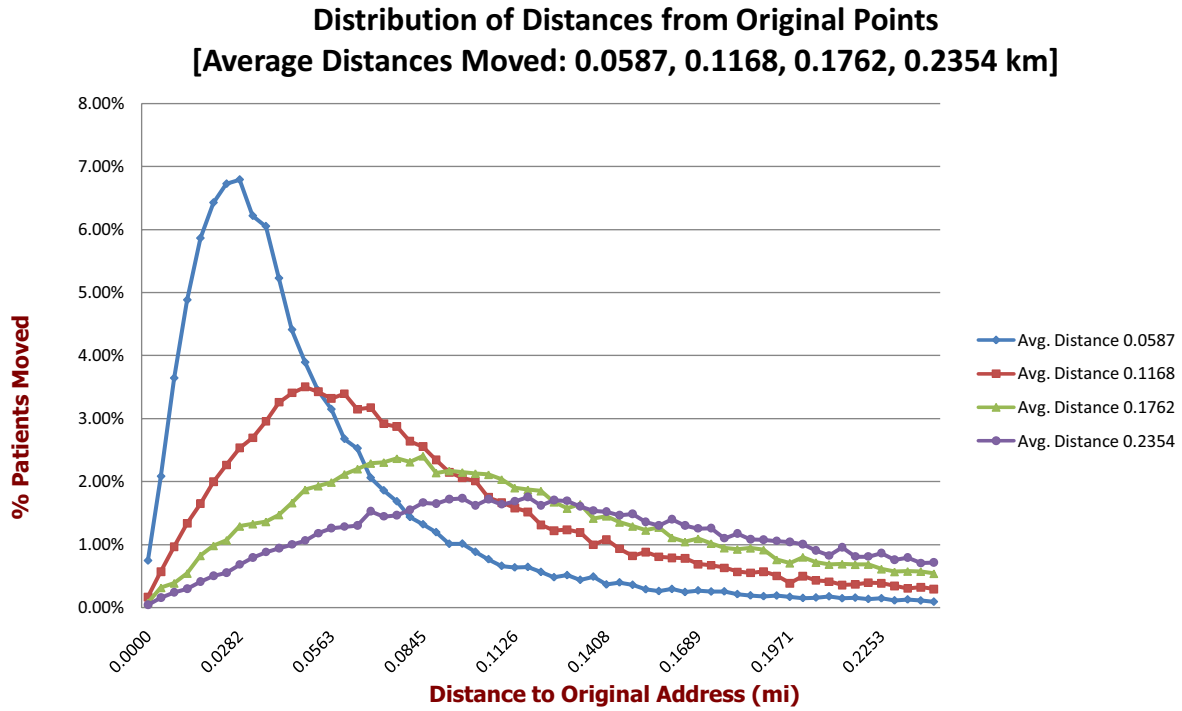
- **Simple aggregation:** Eliminate entire data fields (such as zip code, birth date, street address)
- **Truncation:** Remove portions of those fields (i.e. remove the last two digits of the zip code)
- **Geographically skew:** random changes to geocoded address data
- **Transformation:** Other affine transformations (translations, reflections, dilations preserving colinearity)
- **Geographical aggregation:** K-nearest neighbor 'mixing'

Population Density-Based Anonymization Algorithm

- The goal is to preserve location information without endangering the patient's privacy
- Shifting by 1 mile in a rural area would yield a very different anonymization level than shifting by 1 mile in downtown Manhattan
- Census data can be used to adjust skew of longitudes/latitudes based on population density
- Gaussian weightings and randomizations are used to maintain maximum information while decreasing identifiability

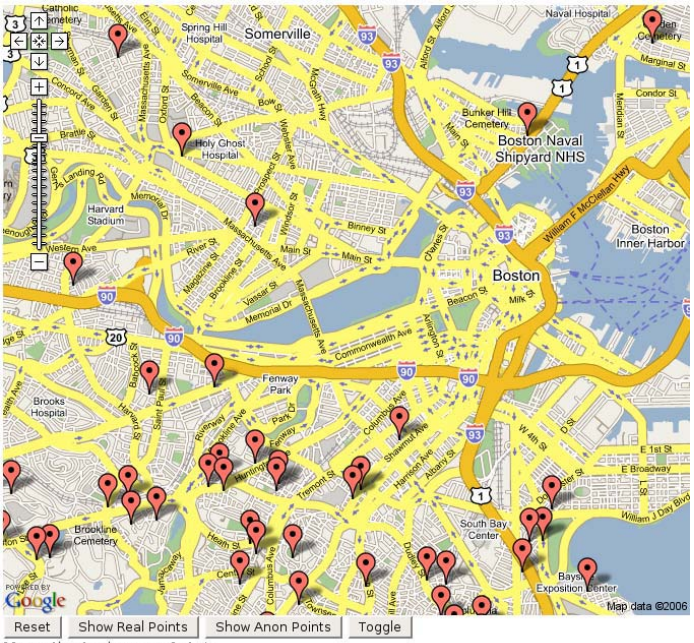
A Gaussian Approach to Anonymization





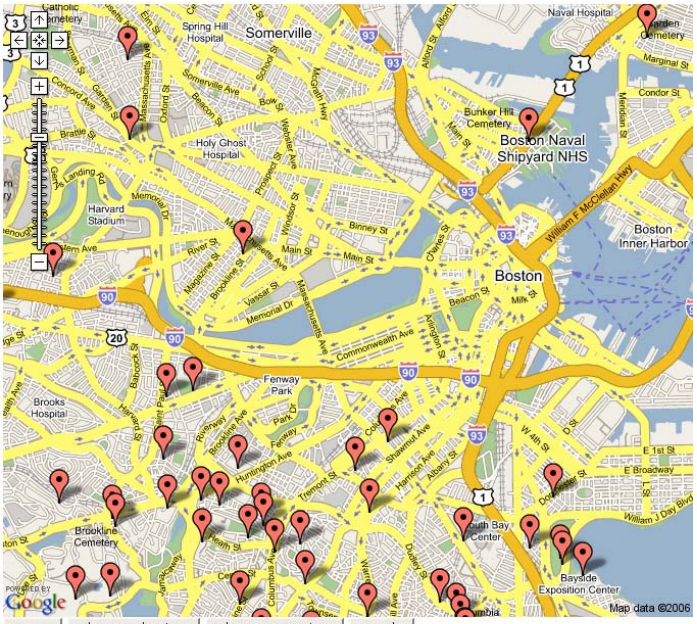
Cassa, Grannis, Overhage, Mandl, JAMIA 2006

Authentic



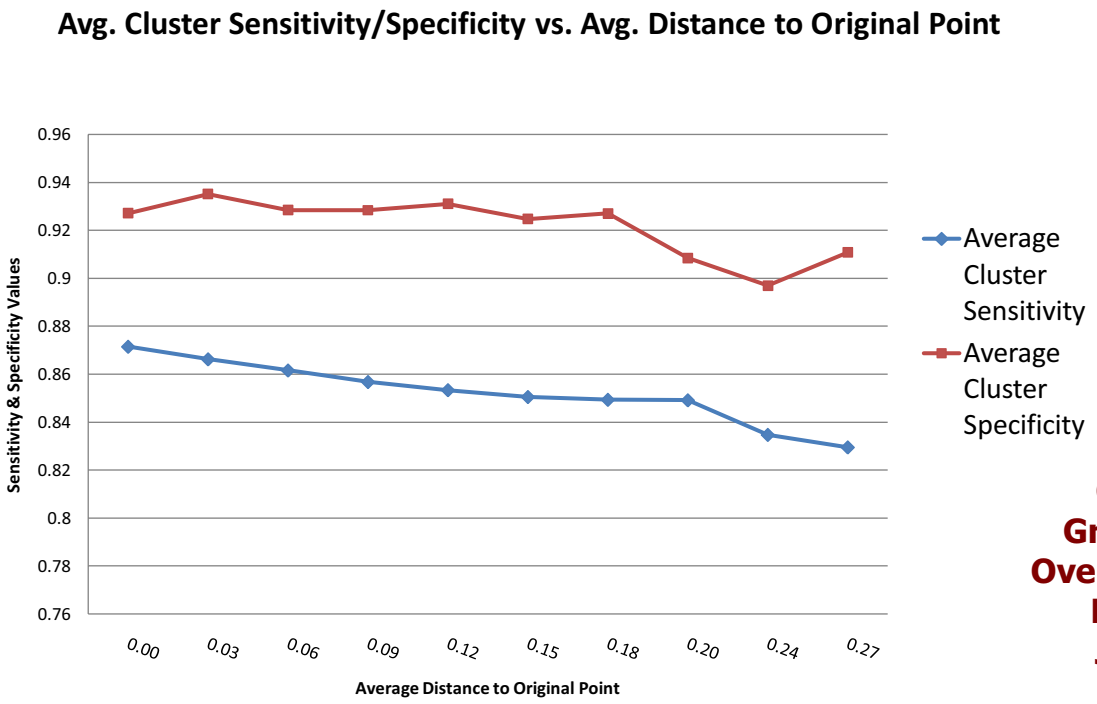
Now displaying **real** data

Anonymized



Now displaying **anonymized** data

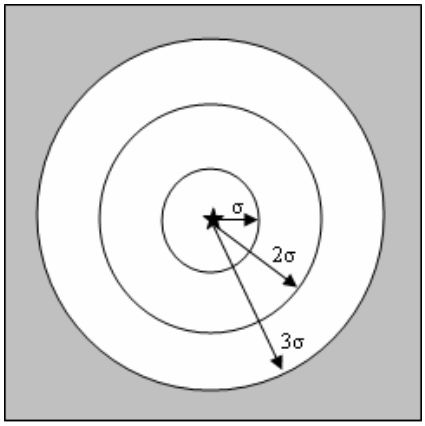
Application Area: Cluster Detection and Disease Surveillance

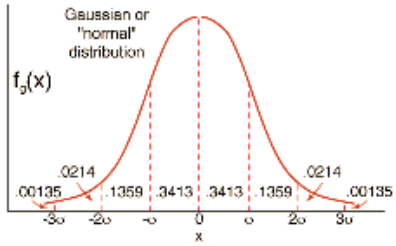


Cassa, Grannis, Overhage, Mandl, JAMIA 2006

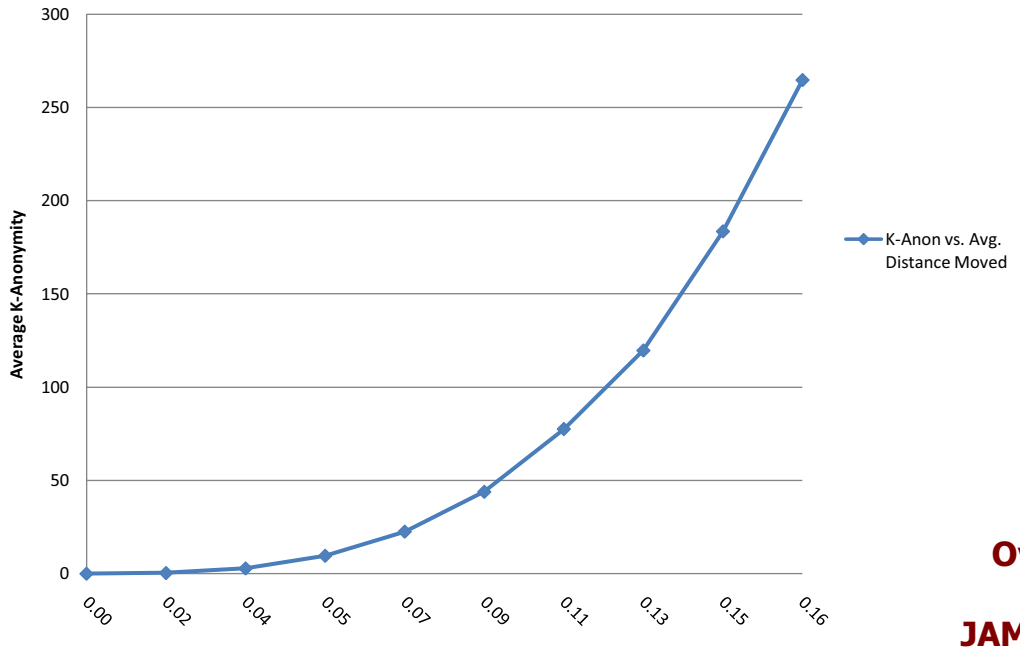
Novel Estimate of K-Anonymity

- 68.26% patients in σ (1SD) miles from center
- Multiply the local population density by the area, $[\pi\sigma_1^2]$
- Then multiply by the probability that the patient would have been moved into that region, 0.6826.
- Repeat each $[\pi(\sigma_n^2 - \sigma_{n-1}^2)]$



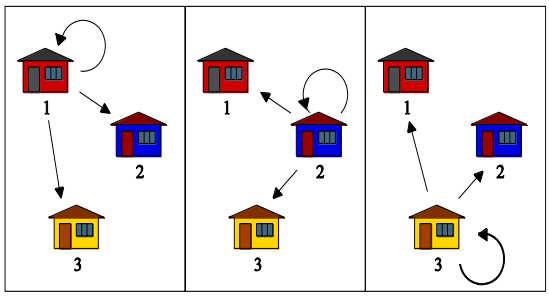


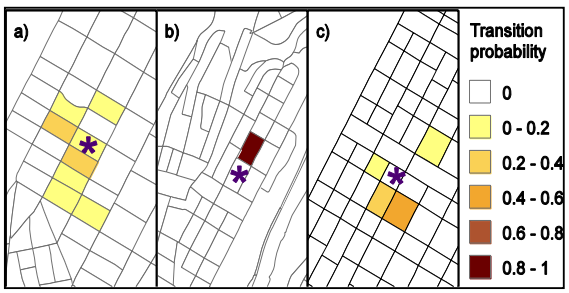
Average *k*-Anonymity Achieved vs. Average Distance Moved [km]



Cassa, Grannis, Overhage, Mandl, JAMIA 2006

Anonymization Using Linear Programming





The decision variables are the transition probabilities P_{ij} of assigning a patient in location $i \in \boldsymbol{A}$ to a new location $j \in \boldsymbol{B}$

Constraint equations specify conditions that must be satisfied by the decision variables P_{ij}.

$$0 \leq P_{ij} \ for\ all\ i \in \boldsymbol{A}\ and\ j \in \boldsymbol{B}$$

In addition, every case must be moved somewhere, so

$$\sum_{j} P_{ij} = 1\ for\ all\ i \in \boldsymbol{A}$$

Constraints

The risk of linking any randomized location with any original patient should be small. We specify the probability that any location from the randomized data set originated from any specific individual in the underlying population is at most ξ:

$$P_{ij} \cdot \frac{n_i}{N} \leq \frac{n_i \cdot \xi}{s} \cdot \sum_{k \epsilon A} \frac{n_k}{N} \cdot P_{kj} \quad for\ all\ i \epsilon \boldsymbol{A}\ and\ j \epsilon \boldsymbol{B}$$

Objective Function is the expected distance that a patient is moved, to be minimized:

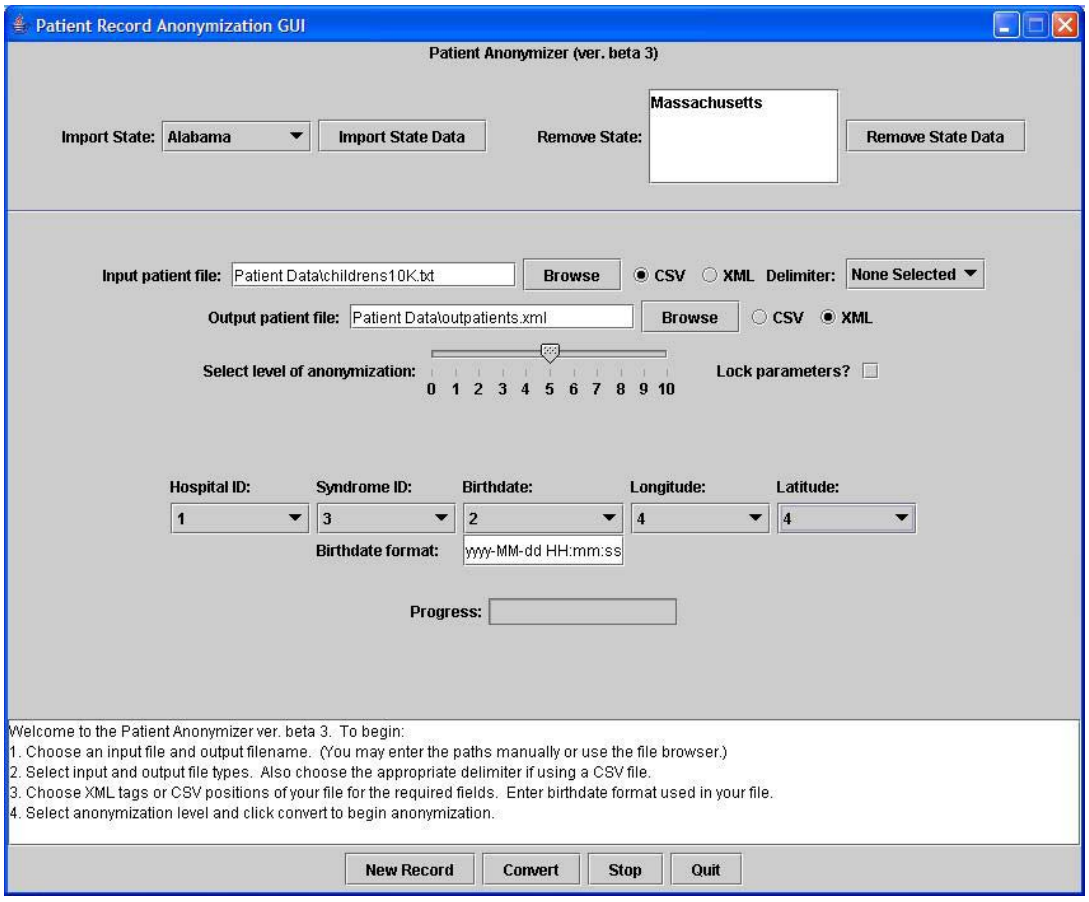
$$\frac{\sum_{i \epsilon A} \sum_{j \epsilon B} d_{ij} \cdot n_i \cdot P_{ij}}{N}$$

Anonymization Using Linear Programming

- Linear programming technique to anonymize address data has several advantages:
  - Finds the mathematically optimal solution
  - Moves points a smaller distance on average
  - No unreasonable locations for points
- Downsides:
  - Most points are not moved very far, so while it is mathematically sound, it may be easy to find cases

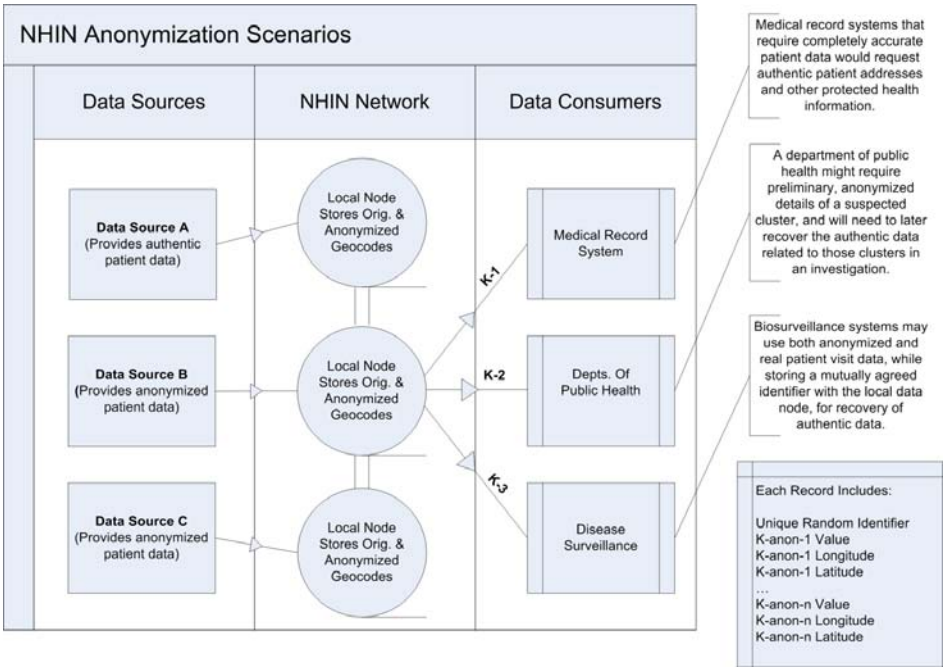
Anonymized Health Data Exchange

- Address data can be anonymized at the data source, so that the data distributed for research and disease surveillance
- Automated open-source tools can handle the conversion at client's location:
  - GUI available for download which handles XML, CSV and soon HL7
  - Core algorithm toolkits being made available for integration with existing infrastructure



Children's Hospital Boston
Informatics Program
Harvard-MIT Division of
Health Sciences and Technology
HST

Automatically Anonymize Data for Dual-Use Health Networks



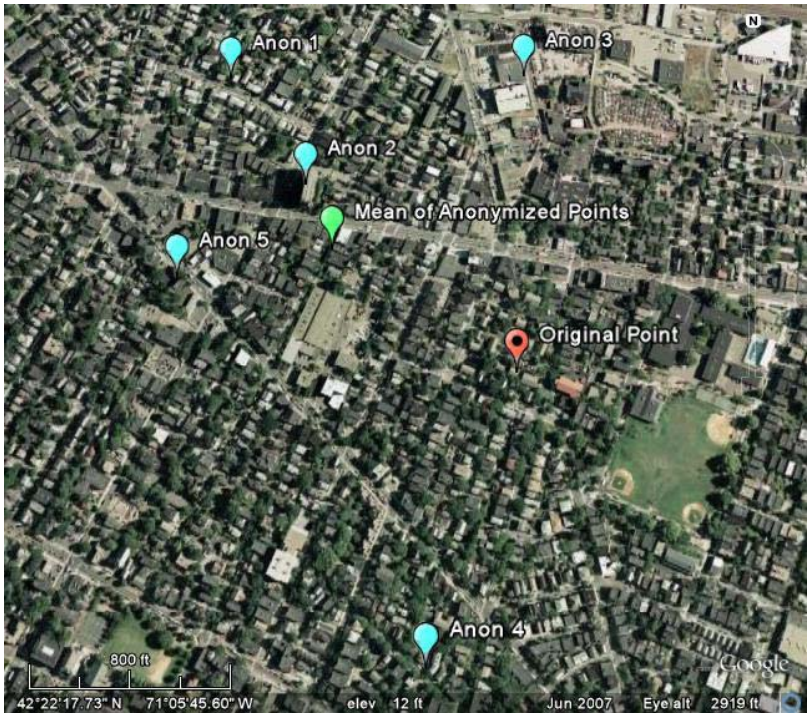
Topics

1. Anonymization of geospatial datasets containing patient home addresses
2. Re-identification potential of geospatial data, commonly shared in both textual form and in printed maps
3. Disclosure risks for genomic data and impact on family members

Anonymization Vulnerabilities

- Explored two classes of anonymization vulnerabilities:
  - Those published in disease maps in journals and in public health practice
  - Those that are more identifiable with multiple versions of the same cases anonymized

Identifying Original Addresses Using Multiple Copies of Anonymized Data



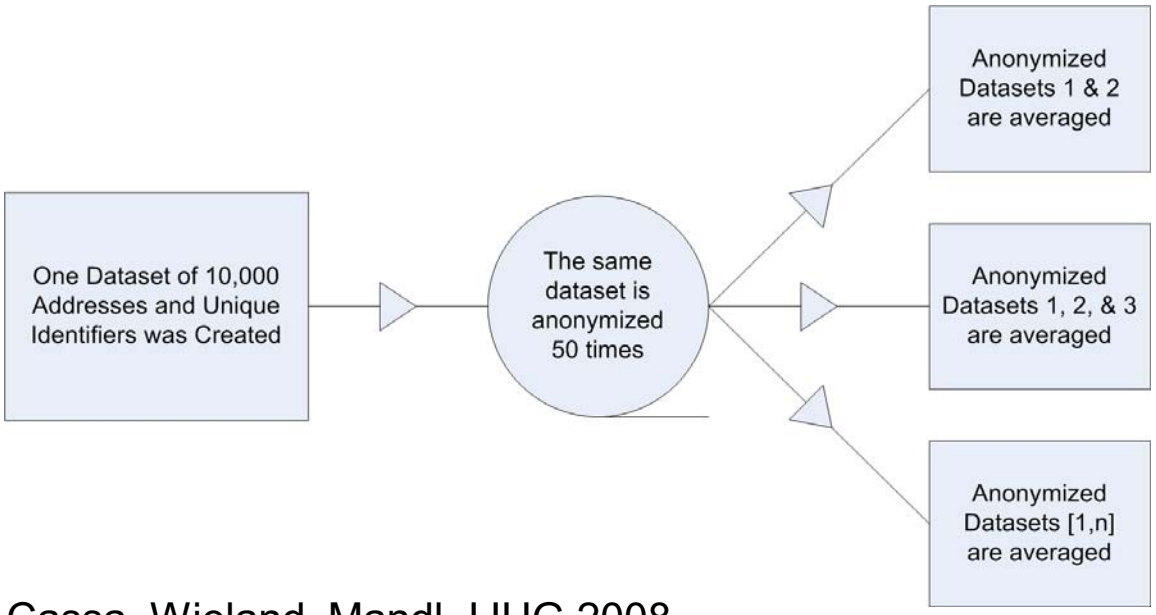
Equivalent of a Less Stringent Anonymization Strategy

The average of *n* anonymized data points with original location $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ is $\frac{\sum_{i=1}^{n} L_i}{n}$; a two-dimensional Gaussian random variable with mean $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ and covariance matrix

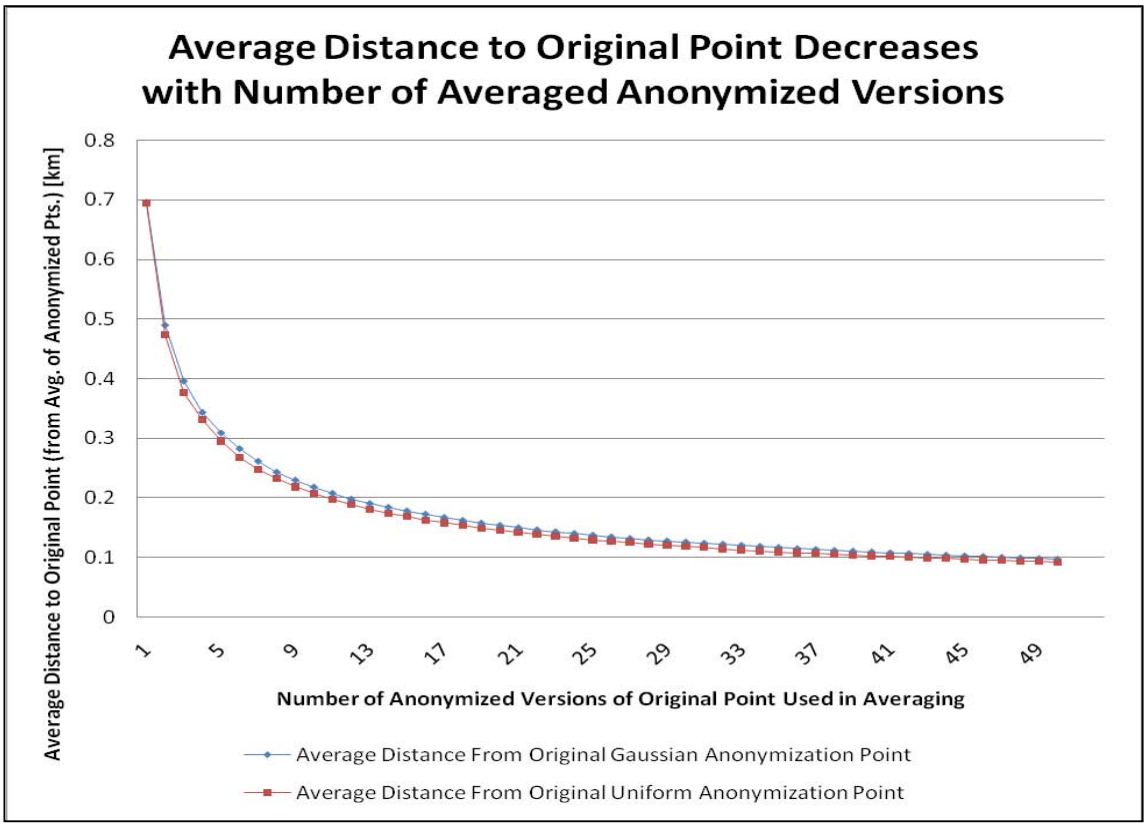
$$\begin{bmatrix} \frac{\sigma^2}{n} & 0 \\ 0 & \frac{\sigma^2}{n} \end{bmatrix}.$$

Inferred data is the same as Gaussian anonymized data with standard deviation of $\sigma/\sqrt{n}$, a less stringent Gaussian skew anonymization level.

Identifying Original Addresses Using Multiple Copies of Anonymized Data



Cassa, Wieland, Mandl. IJHG 2008



Cassa, Wieland, Mandl. IJHG 2008

Next Steps

- Geographical Constraints (both physical and demographic) for anonymized point distribution
- Pre-anonymization detection to geographically constrain points
- Integration of other anonymizing methods for non-spatial data types

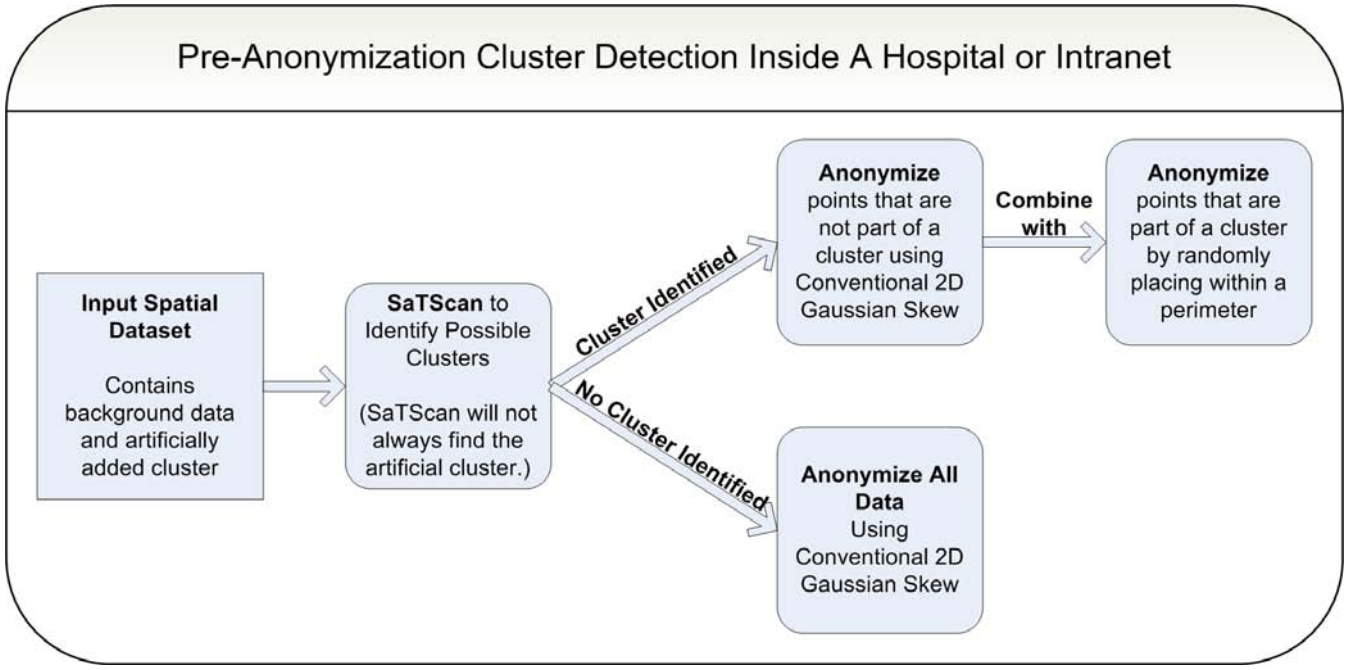
New Research: Constraining Geographic Distribution of Points

- Points are sometimes placed on mountains and lakes or in other regions that are otherwise inappropriate for placement
- Is it possible to geographically constrain the placement of some points without upsetting the distribution of all cases
- Can privacy be assured if the distribution shape changes?

New Research: Pre-Anonymization Detection

- Is it possible to detect potential clusters before anonymizing cases and then geographically constrain points?
- Cluster points would be distributed within a smaller boundary so that they will be more easily detectable after anonymization
- This should improve detection rates of small clusters in anonymized data that would otherwise be blurred too much

Pre-Anonymization Detection



Topics

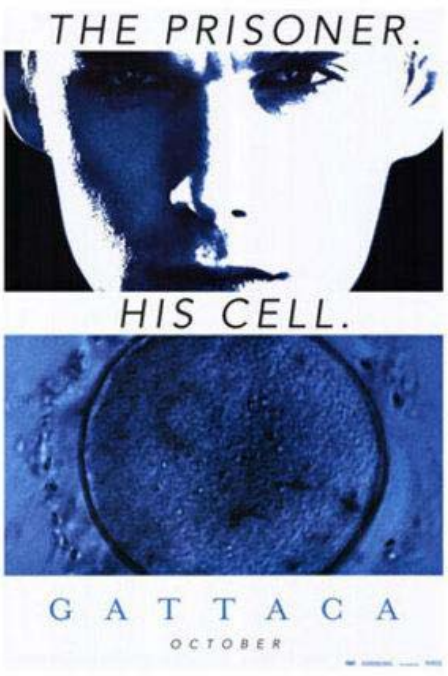
1. Anonymization of geospatial datasets containing patient home addresses
2. Re-identification potential of geospatial data, commonly shared in both textual form and in printed maps
3. Disclosure risks for genomic data and impact on family members

Data Rapidly Becoming Available

- Research studies publish sequencing and expression data for other investigators
- Public Studies:
  - HapMap Study
  - NHLBI GWAS Framingham & Jackson Studies
- Available to the public at large

23andMe Navigenics deCODE ME Knome

Broad Fear of DNA Use in Society



What Protections are in Place?

- Genetic Information Non-Discrimination Act
  - Passed in 2008
- State Laws Protecting Similar Items

Genomic Data Pose Unique Risks

- Discrimination Concerns
  - Insurance, workplace discrimination
  - Life, disability, and long term care insurance uncovered
- Genetic Knowledge and Personal Decision Making
- Implications for family members

Why Risk GATTACA?

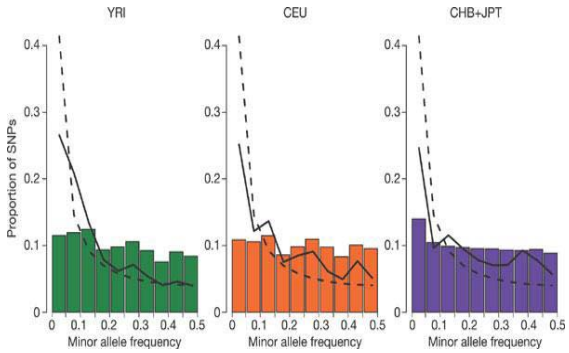
- Correlate clinical outcomes with genomic data
- Individual participation necessary – sharing genotypic and clinical data with investigators
- Methods to help individuals with risk assessment and to preserve privacy with such disclosures needed

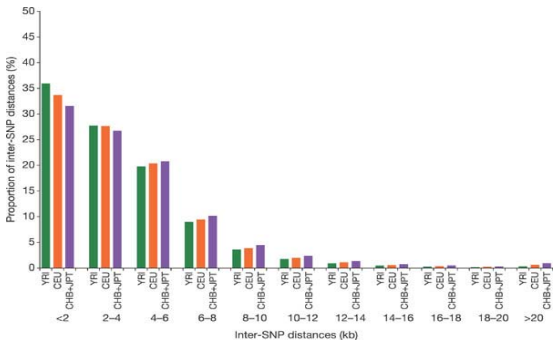
Risk Disclosure Models

- Risk of Identity Linkage
- Risk of Aggregation
- Risk of Phenotypic Linkage
- Risk of Familial Linkage

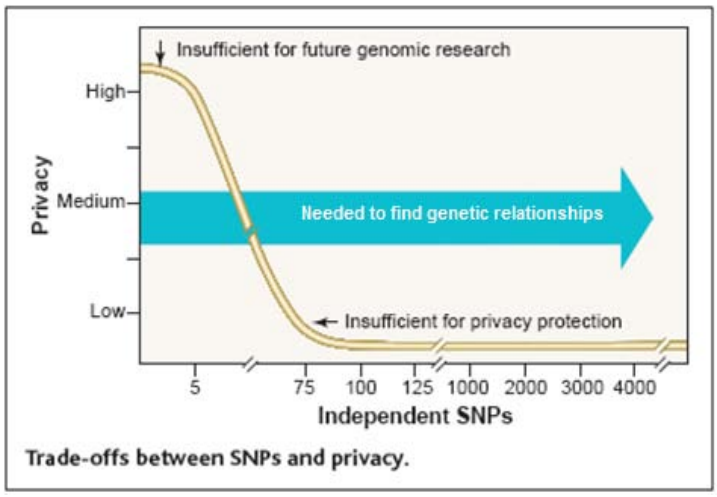
Background

- Single Nucleotide Polymorphisms (SNPs) are genetic locations where at least 1% of the population has a different base pair
- SNPs distributed throughout the genome, responsible for much genetic diversity





Risk of Identity Linkage: Privacy Decreases Sharply with a Small Set of SNPs



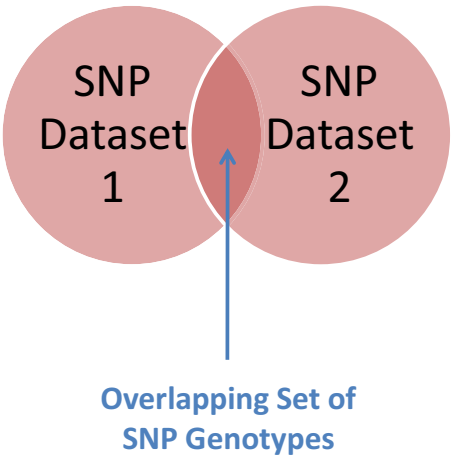
Trade-offs between SNPs and privacy.

- At a low number (35-70) of identified **independent** SNPs, the amount of privacy dramatically decreases.
- Match a hair or a soda can to a record.

Genomic Research and Human Subject Privacy

Zhen Lin, Art B Owen, Russ B Altman. Science. Vol.305, Iss. 5681; pg. 183

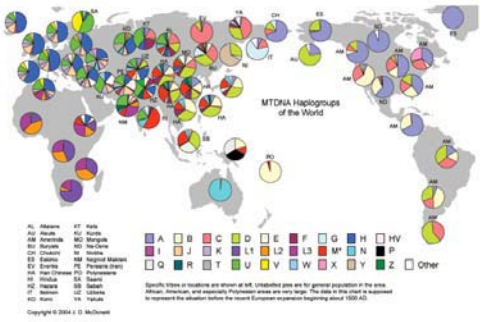
Risk of Aggregation: Combining Two Separate Genomic Datasets

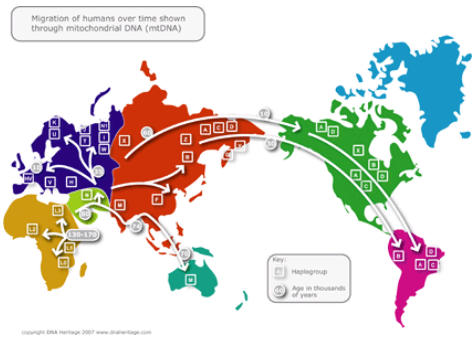


- Extension of Risk of Identity Linkage
- With an overlapping set of SNPs and *no* supporting information, can one identify the whether two datasets came from one person?

Risk of Phenotypic Linkage: Identifying Phenotypes from Genotypes (and vice versa)

- Genomic data never "unlinked" to identity
  - Gender
  - Race/Ethnicity
  - Other physical characteristics
  - Propensity for diseases



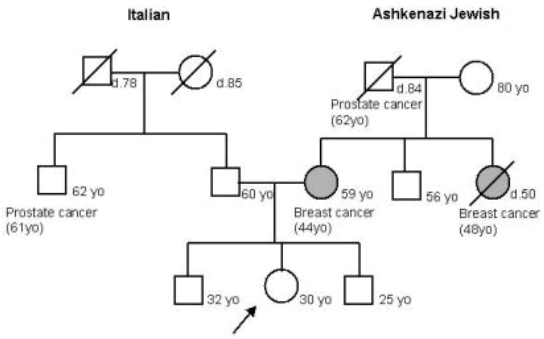


B. Malin and L. Sweeney. *Inferring Genotype from Clinical Phenotype Through a Knowledge-based Algorithm.* Pacific Symposium on Biocomputing Jan 2002: 41-52.

Risk of Familial Linkage

- Siblings share 50% of contiguous chromosomal segments, and a larger fraction of genotypes
- We share 25% of our DNA with our grandparents, aunts and uncles, and 12.5% with first cousins

With your genomic data how many SNP values can be identified for Parents, Siblings & Children



No Genomic Privacy: Protective Strategies Inadequate

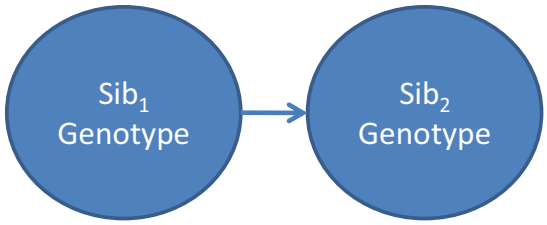
- Using Binning to Maintain Confidentiality
- Disclosing Aggregate Data (Frequencies)
- Use of Generalization Lattices
- Adding Noise to Genetic Data
- Creating Synthetic Individuals
- Anonymization by Pool Selection

Genomic Data in Medical Records

- **SNPs**
- Mutations
- Any DNA Sequencing
- Race/Ethnicity
- Family History Data, including Genetic Diagnoses
- Phenotypic clinical data including diseases and allergies
- Gene expression Profiles
- Proteomics Data
- More to come…

Genomic Inference: Identifying Sibling Genotypes

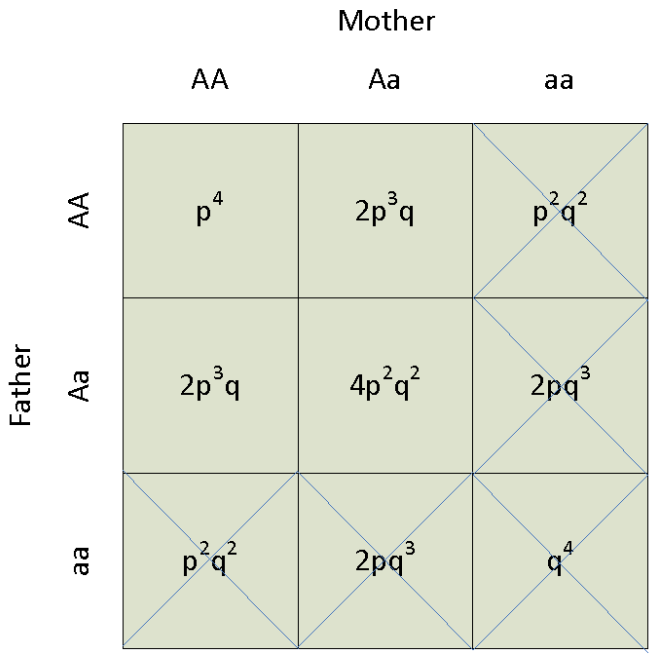
- Improving genotype inferences using Sib_1 genotype at one SNP (extensible to families)
- Confirming sibling relationship given matches at sets of SNP loci
- Measuring information provided by knowledge of Sib_1 genotype
- Relative risk for carrying a minor allele
- Experimental results



Children's Hospital Boston
Informatics Program
Harvard-MIT Division of
Health Sciences and Technology
HST

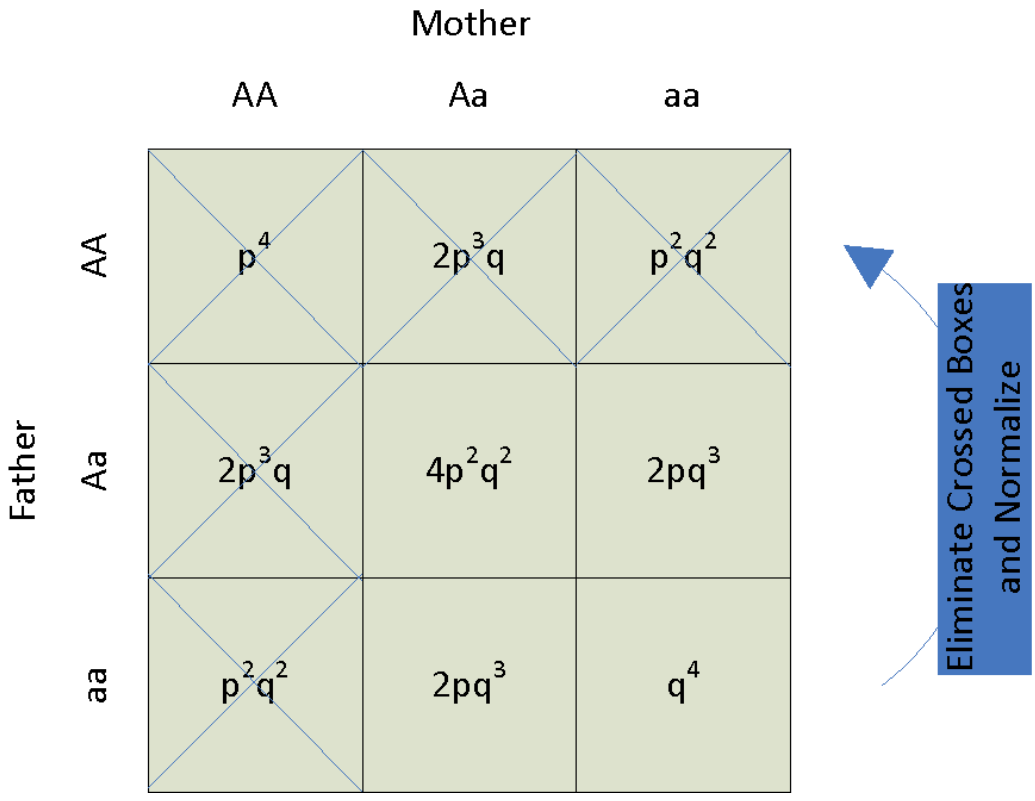
Improving Genotype Inferences Using Sib_1 genotype at One SNP

First sib is homozygous major at SNP A

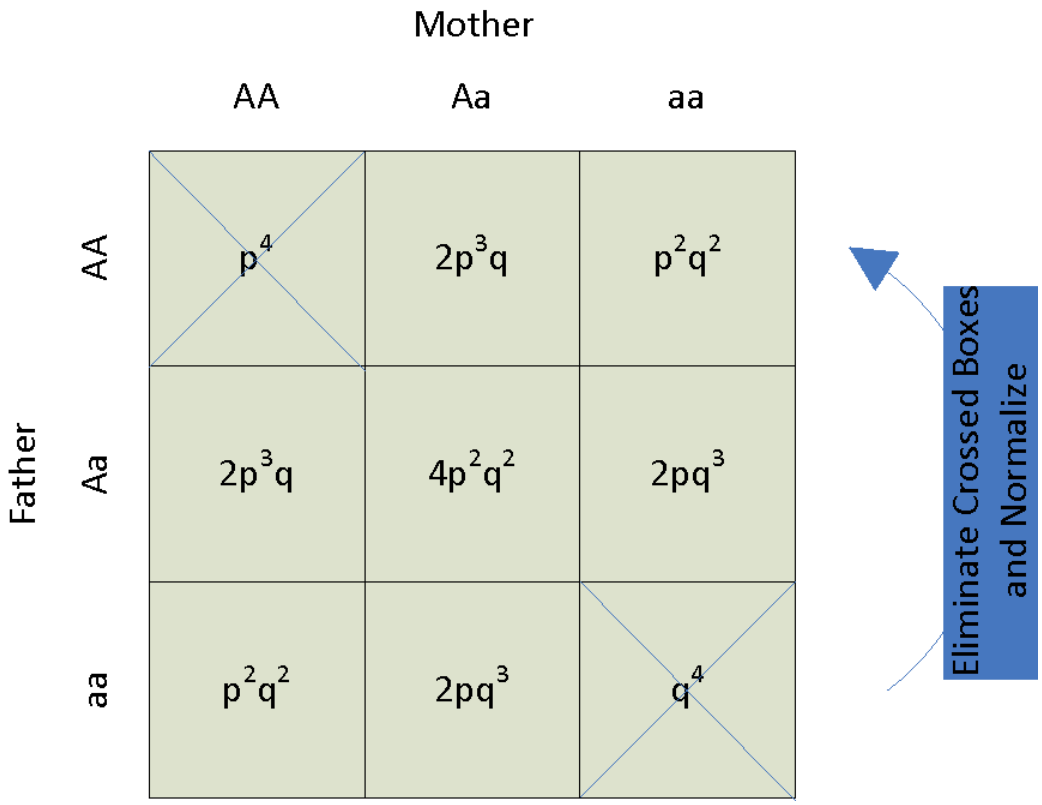


For example, when Sib1 is homozygous major, all possible parental genotypic candidates that involve one or both parent genotypes of *'aa'* are excluded, as it is not possible to have a child with genotype *'AA'* if either parent does not have at least one copy of the *'A'* allele.

First sib is homozygous minor at SNP A



First sib is heterozygous at SNP A



Calculating $p(Sib_2AA|Sib_1AA)$ for one SNP

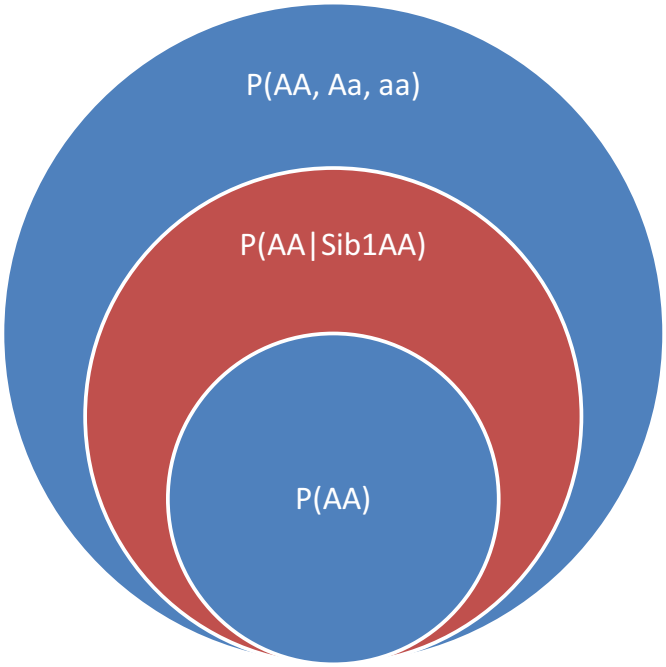
Nine possible parental genotypic combinations (*i*) at each SNP:

$$p(Sib_2AA|Sib_1AA) = \sum_{i=1}^{9} p(Sib_2AA|parental\ comb.\ i)p(parental\ comb.\ i|\ Sib_1AA)$$

$$= \sum_{i=1}^{9} \left(\frac{p(Sib_2AA \cap parental\ comb.\ i)}{p(parental\ comb.\ i)} \right) p(parental\ comb.\ i|\ Sib_1AA)$$

Sib_1AA and Sib_2AA refer to Sib 1 and Sib 2 genotypes *'AA'*, at the SNP in question, using HapMap SNP population frequencies, p and q for the SNP being evaluated.

Increase in Accuracy from Sib_1 Knowledge



The red section in the overlapping Venn diagram is the improvement from knowledge of the Sib_1 genotype in making the Sib_2 genotype inference.

Example: Calculating $p(Sib_2AA|Sib_1AA)$

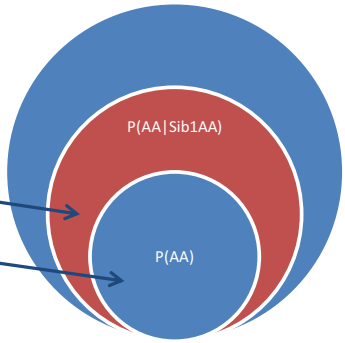
$$= \sum_{i=1}^{4} \left(\frac{p(Sib_2AA \cap parental\ comb.\ i)}{p(parental\ comb.\ i)} \right) p(parental\ comb.\ i | Sib_1AA)$$

$$= \left(\frac{p(Sib_2AA \cap AA_MAA_F)}{p(AA_MAA_F)} \right) p(AA_MAA_F|Sib_1AA) + \left(\frac{p(Sib_2AA \cap AA_MAa_F)}{p(AA_MAa_F)} \right) p(AA_MAa_F|Sib_1AA)$$
$$+ \left(\frac{p(Sib_2AA \cap Aa_MAA_F)}{p(Aa_MAA_F)} \right) p(Aa_MAA_F|Sib_1AA) + \left(\frac{p(Sib_2AA \cap Aa_MAa_F)}{p(Aa_MAa_F)} \right) p(Aa_MAa_F|Sib_1AA)$$

$$= (1)(p^2) + \left(\frac{1}{2}\right)(pq) + \left(\frac{1}{2}\right)(pq) + \left(\frac{1}{4}\right)(q^2)$$

$$= p^2 + pq + \frac{q^2}{4}$$

$$= p^2 + \left[pq + \frac{q^2}{4} \right]$$



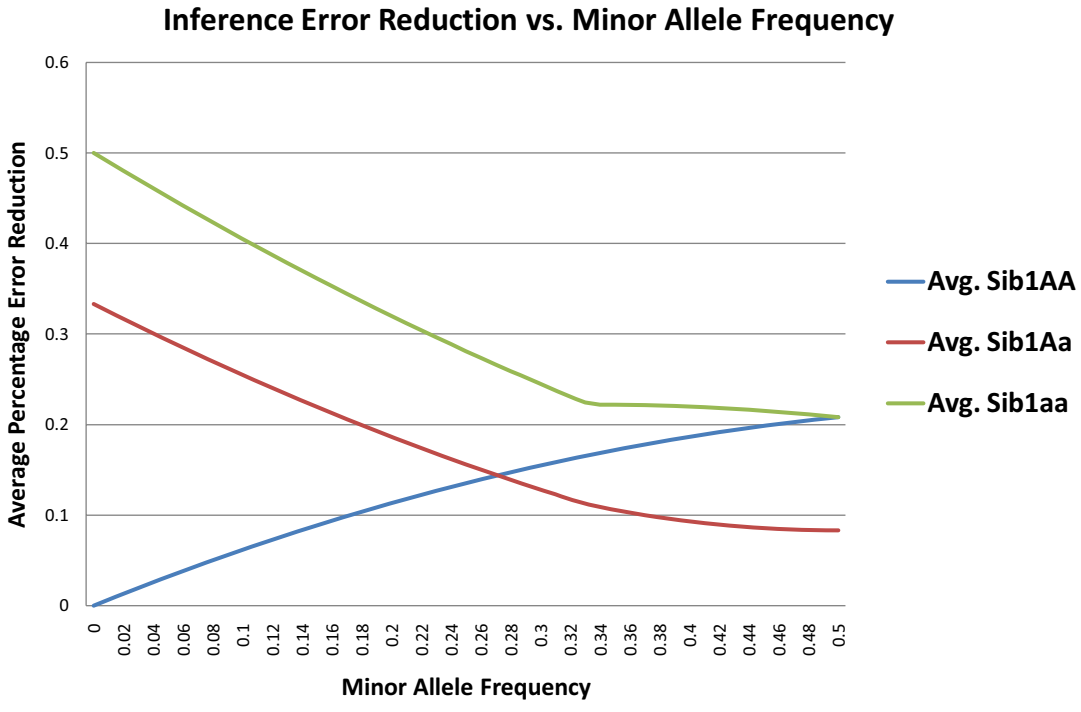
Example: Calculating $p(Sib_2X|Sib_1Y)$

- Using the same technique, we can calculate all possible $p(Sib_2X|Sib_1Y)$
- Prior probability is Hardy-Weinberg equilibrium value
- Posterior includes knowledge of Sib_1 genotype

Sib_2	Sib_1	Prior Prob.	Posterior Prob.	Error Reduction
AA	AA	p^2	$p^2 + pq + \frac{1}{4}q^2$	$\lvert p^2 - [p^2 + pq + \frac{1}{4}q^2]\rvert$
Aa	AA	2pq	$pq + \frac{1}{2}q^2$	$\lvert 2pq - [pq + \frac{1}{2}q^2]\rvert$
aa	AA	q^2	$\frac{1}{4}q^2$	$\lvert q^2 - [\frac{1}{4}q^2]\rvert$
AA	Aa	p^2	$\frac{1}{2}p^2 + \frac{1}{4}pq$	$\lvert p^2 - [\frac{1}{2}p^2 + \frac{1}{4}pq]\rvert$
Aa	Aa	2pq	$\frac{1}{2}p^2 + (\frac{2}{3})^{-1}pq + \frac{1}{2}q^2$	$\lvert 2pq - [\frac{1}{2}p^2 + (\frac{2}{3})^{-1}pq + \frac{1}{2}q^2]\rvert$
aa	Aa	q^2	$\frac{1}{4}pq + \frac{1}{2}q^2$	$\lvert q^2 - [\frac{1}{4}pq + \frac{1}{2}q^2]\rvert$
AA	aa	p^2	$\frac{1}{4}p^2$	$\lvert p^2 - [\frac{1}{4}p^2]\rvert$
Aa	aa	2pq	$\frac{1}{2}p^2+pq$	$\lvert 2pq - [\frac{1}{2}p^2+pq]\rvert$
aa	aa	q^2	$\frac{1}{4}p^2 + pq + q^2$	$\lvert q^2 - [\frac{1}{4}p^2 + pq + q^2]\rvert$

Cassa, Kohane, Mandl, BMC Medical Genomics 2008

Avg. Error Reduction by Sib_1 Genotype



Measuring Information Provided by Knowledge of Sib_1 Genotype

Measure information provided by knowledge of Sib_1 genotype using the ratio between the inference with knowledge and without:

$$\Lambda_{Ind_1, Ind_2\ genotypes} = \frac{p(Ind_2 genotype | Ind_1 genotype \cap siblings)}{p(Ind_2 genotype | Ind_1 genotype \cap unrelated)}$$

The log of this odds ratio can then be used as a statistic for measuring relatedness, depending only on the SNP allele frequency and the Sib_1 genotype

Probabilistic Maneuvering

$$\Lambda_{Ind_1, Ind_2\ genotypes} = \frac{p(Ind_2 genotype | Ind_1 genotype \cap siblings)}{p(Ind_2 genotype | Ind_1 genotype \cap unrelated)}$$

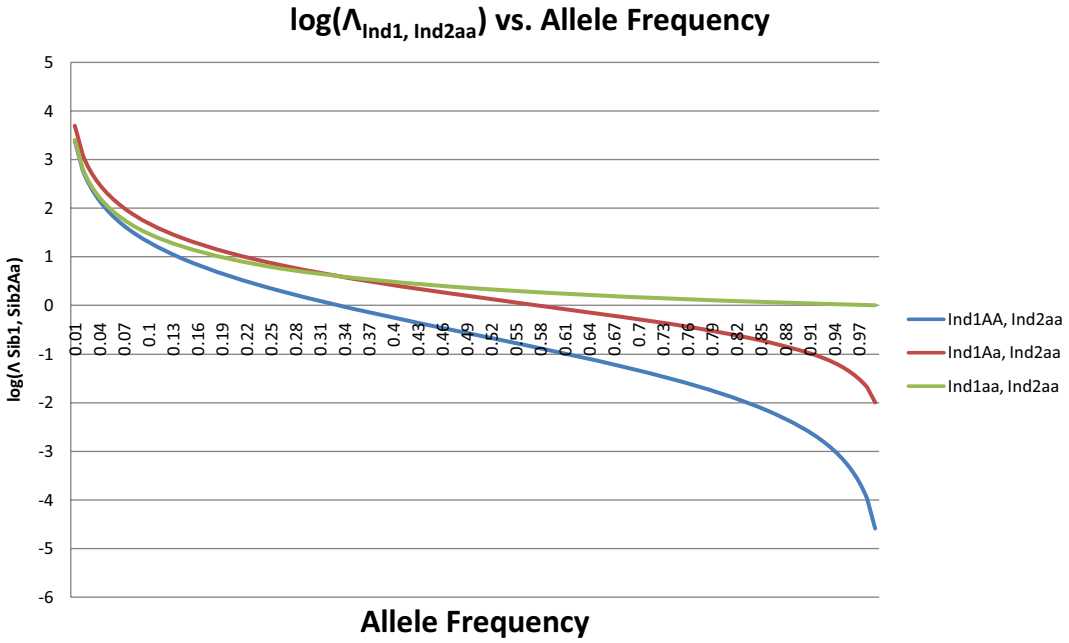
$$= \frac{p(Sib_2 genotype | Sib_1 genotype)}{\left(\frac{p(Ind_2 genotype) \cap p(Ind_1 genotype \cap unrelated))}{p(Ind_1 genotype \cap unrelated)}\right)}$$

$$= \frac{\sum_{i=1}^{9} p(Sib_2 genotype | parental\ comb.i) p(parental\ comb.i | Sib_1 genotype)}{\left(\frac{p(Ind_2 genotype) \cap p(Ind_1 genotype \cap unrelated))}{p(Ind_1 genotype \cap unrelated)}\right)}$$

$$= \frac{\sum_{i=1}^{9} \left(\frac{p(Sib_2 genotype \cap parental\ comb.i)}{p(parental\ comb.i)}\right) p(parental\ comb.i | Sib_1\ genotype)}{\left(\frac{p(Ind_2 genotype) \cdot p(Ind_1 genotype) \cdot \left(1 - \frac{1}{N}\right)}{p(Ind_1 genotype) \cdot \left(1 - \frac{1}{N}\right)}\right)}$$

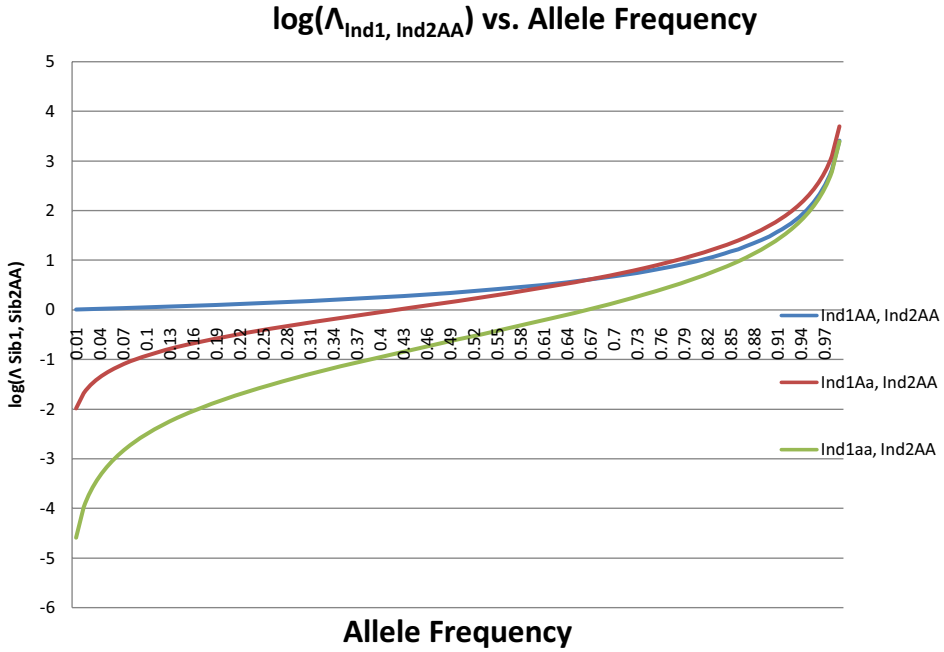
$$\cong \frac{\sum_{i=1}^{9} \left(\frac{p(Sib_2 genotype \cap parental\ comb.i)}{p(parental\ comb.i)}\right) p(parental\ comb.i | Sib_1\ genotype)}{p(Ind_2 genotype)}$$

Measuring Information Provided by Knowledge of Sib_1aa Genotype



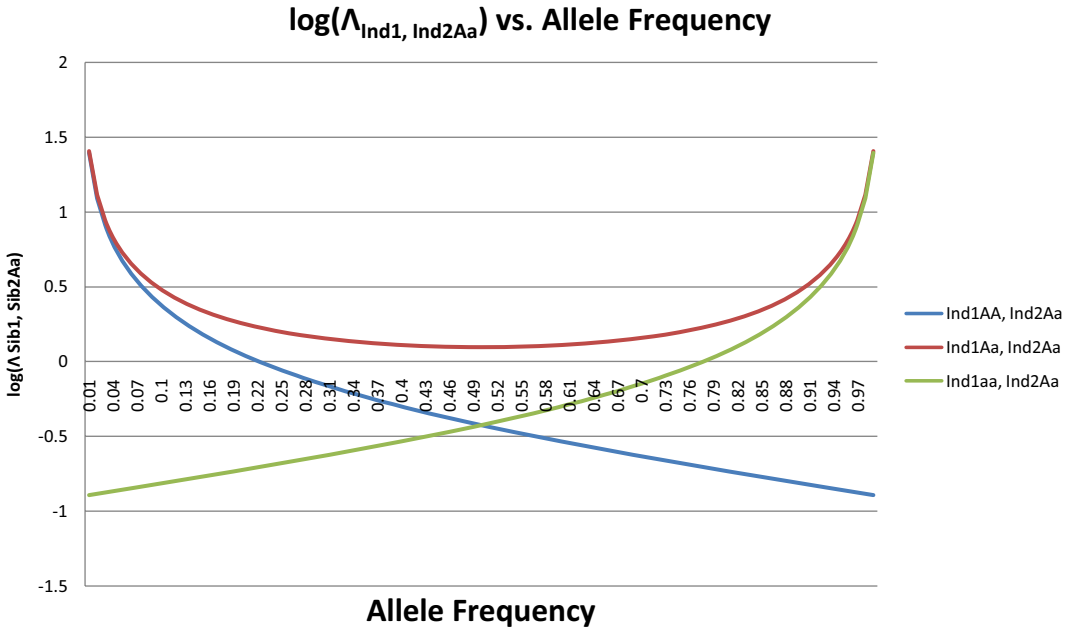
Cassa, Kohane, Mandl. BMC Medical Genomics 2008

Measuring Information Provided by Knowledge of Sib_1AA Genotype



Cassa, Kohane, Mandl. BMC Medical Genomics 2008

Measuring Information Provided by Knowledge of Sib_1Aa Genotype



Cassa, Kohane, Mandl. BMC Medical Genomics 2008

Confirming Sibling Relationship Given Matches at SNP Loci

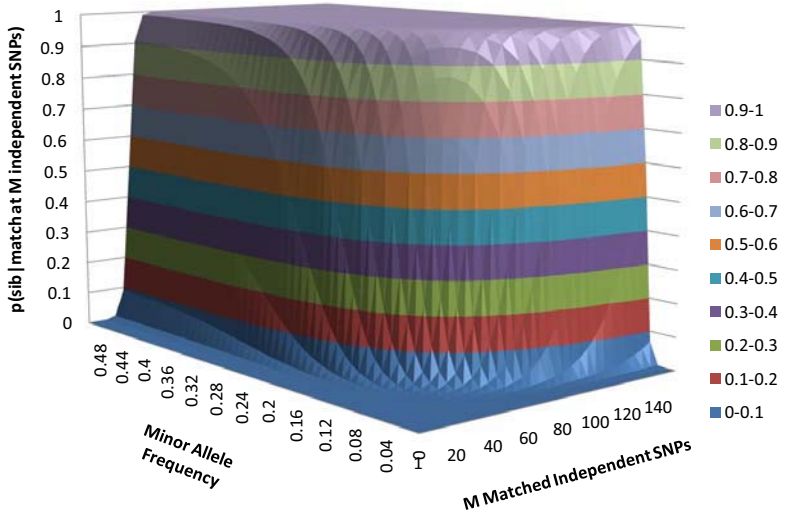
• Probability that two people in a pool of size *N* are siblings calculated using a version of Bayes' Theorem, if they have matching alleles at *M* independent SNP loci.

$$p(sibs|match\ at\ M\ loci) = \frac{p(match\ at\ M\ loci|sibs)\ p(sibs)}{p(match\ at\ M\ loci|sibs)p(sibs) + p(match\ at\ M\ loci|!\,sibs)p(!\,sibs)}$$

$$= \frac{[p(both\ AA|sibs) + p(both\ Aa|sibs) + p(both\ aa|sibs)]^M \left(\frac{1}{N}\right)}{[p(both\ AA|sibs) + p(both\ Aa|sibs) + p(both\ aa|sibs)]^M \left(\frac{1}{N}\right) + p(match|!\,sibs)^M \left(1 - \frac{1}{N}\right)}$$

Confirming Sibling Relationship Given Matches at SNP Loci

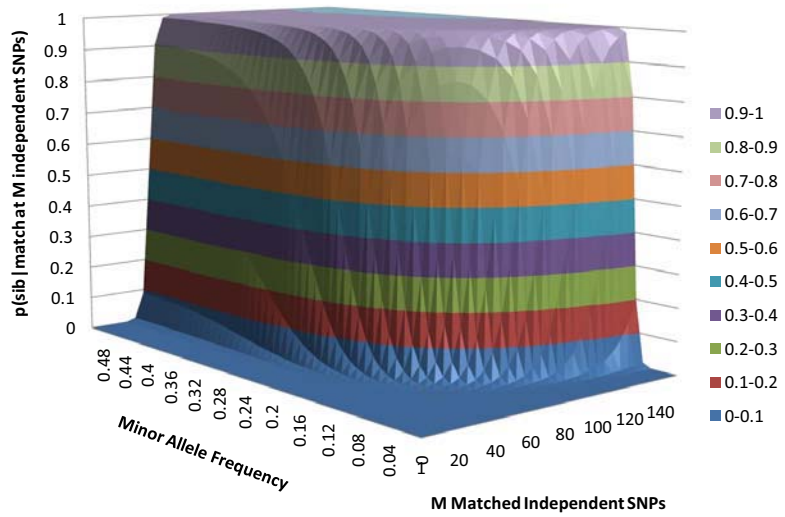
[a] p(sib | match at M independent SNPs) vs. Minor Allele Frequency (N=100,000)



Cassa, Kohane, Mandl. BMC Medical Genomics 2008

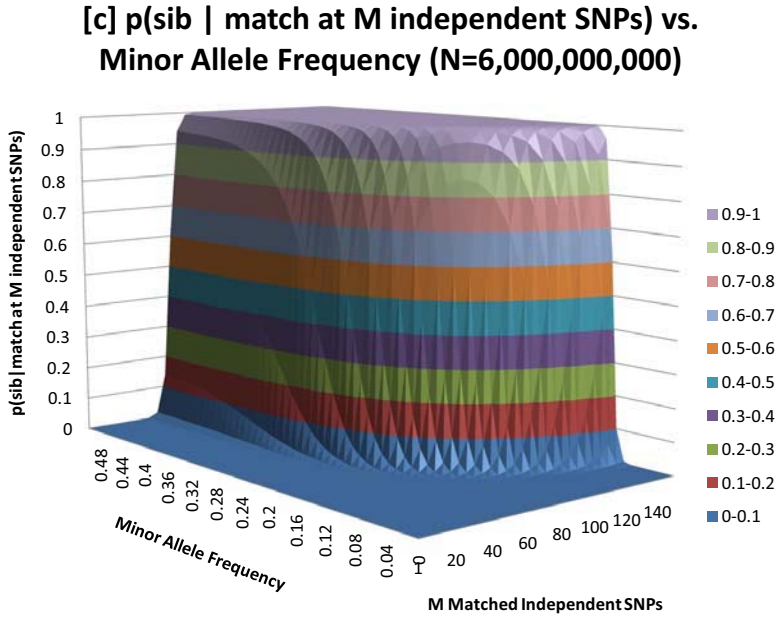
Confirming Sibling Relationship Given Matches at SNP Loci

[b] p(sib | match at M independent SNPs) vs. Minor Allele Frequency (N=10,000,000)



Cassa, Kohane, Mandl. BMC Medical Genomics 2008

Confirming Sibling Relationship Given Matches at SNP Loci



Cassa, Kohane, Mandl. BMC Medical Genomics 2008

How Many Genotypic Inferences Should We Expect to Get Correct?

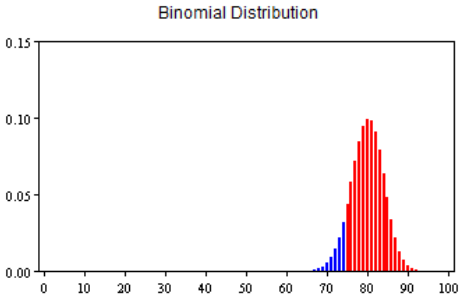
- Guesses can be treated as a random variable with *p* as the average % of success, as long as SNPs selected are independent.
- If *n* guesses are considered (i.e. *n* SNPs are genotyped and used for sib inference), what is the probability that *k* of those will be correct,

$$p(k,n,p) = \binom{n}{k} p^k (1-p)^{n-k}$$

$$F(k;n,p) = P(X \le k) = \sum_{j=0}^{k} \binom{n}{j} p^j (1-p)^{n-j}$$

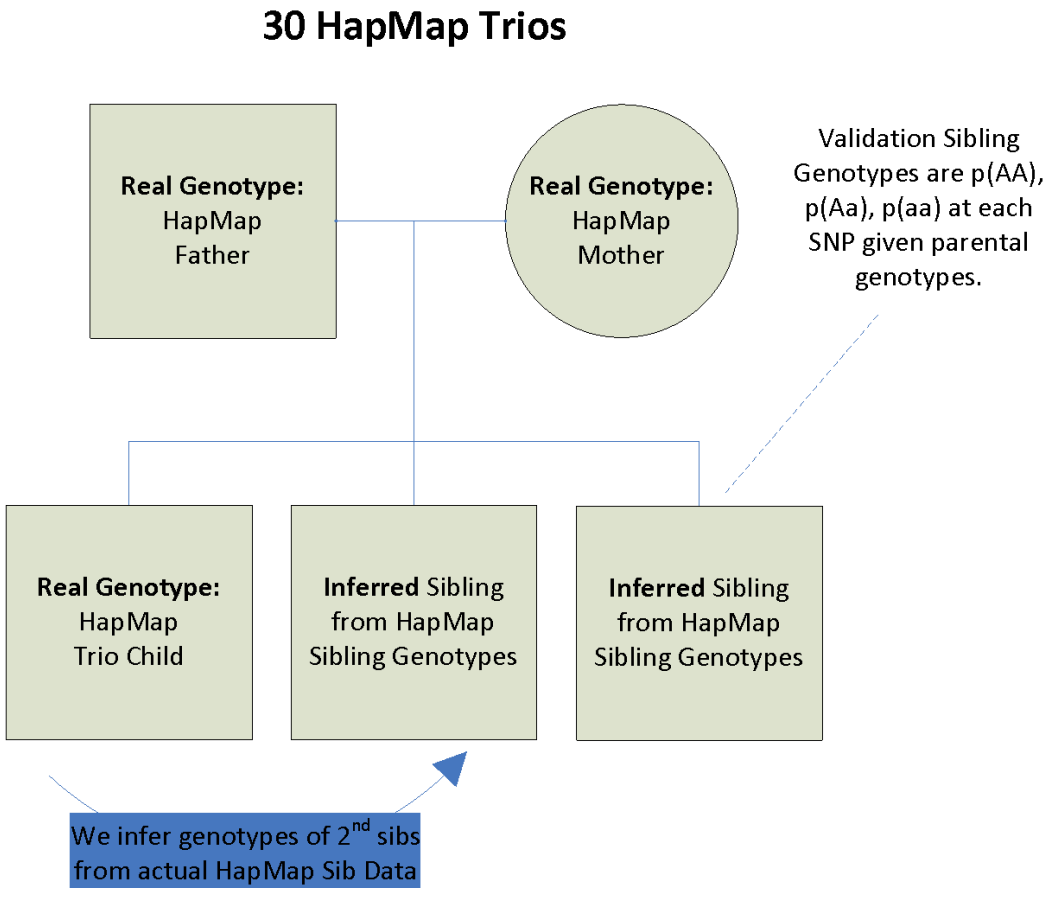
Example: *n* = 100 SNP inferences, *p* = 0.8 of correct inferences

What is the probability of at least *k* = 75 correct guesses



Inference Experimental Results

- 700,000 SNPs on 3 chromosomes (2,4,7), 30 HapMap CEPH trio datasets were used.
- For each SNP, the child's genotype was used to infer the genotype of another sib at that locus using a refining strategy and SNP population frequencies.
- Results were validated using the expected probabilities p(AA), p(Aa), p(aa) of children from the parents in the HapMap trios.



Scoring Genotypic Inferences

- Results come in the form of:
  - *p(AA), p(Aa), p(aa)* for the inferred sibs
- Validation data comes in the form of:
  - *p(AA), p(Aa), p(aa)* given actual parent gtype.
- If we 'called' the correct expected genotype, we get a full point.
- If we 'called' one of the two matched 0.5/0.5 genotypes we get a half point.

Results of Genomic Inferences

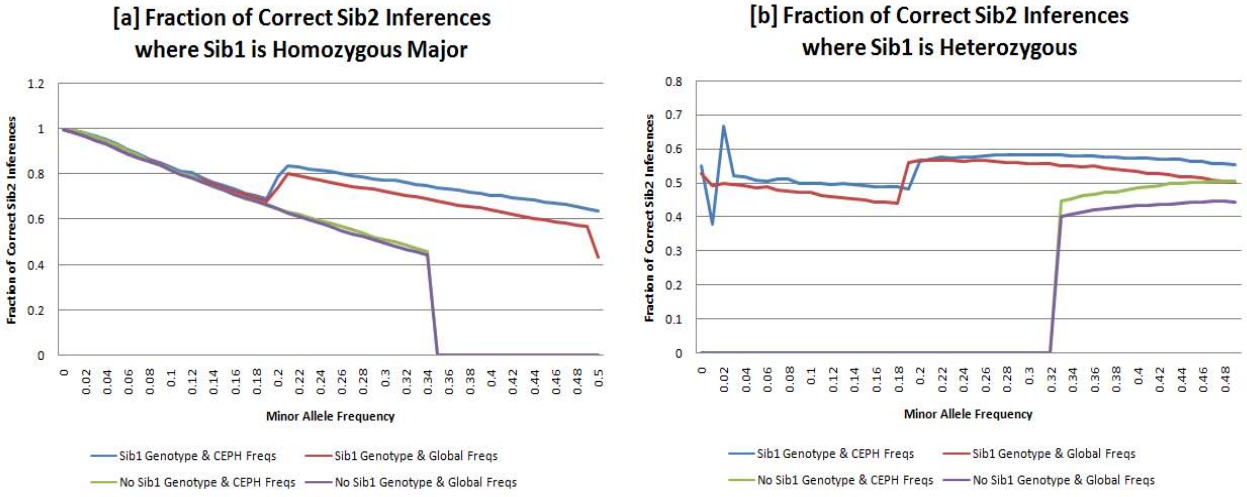
For SNPs where Sib_1 was **homozygotic major:**

- Minor allele frequency < 0.05 (N=300512,43.2%), we can infer Sib_2 with 98.5% accuracy
- Minor allele frequency < 0.20 (N=452684, 65.1%), we can infer Sib_2 with 91.9% accuracy

For SNPs where Sib_1 was **heterozygotic:**

- Minor Allele Frequency > 0.20 (N=125796, 18.1%), it is possible to infer the correct genotype of the second sibling with 57.7% average accuracy.

Percentage of Correct Inferences



Cassa, Kohane, Mandl. BMC Medical Genomics 2008

Relative Risk for Sibling Carrying a Specific Genotype

Sibling SNP data can be used to quantify an individual's disease propensity through genotypic inference, without that individual's actual sequence data

$$\Gamma_{Sib_2\ genotype\ \ |Sib_1\,genotype} = \frac{\text{probability with sibling knowledge}}{\text{probability without sibling knowledge}}$$

$$= \frac{p(Sib_2\,genotype|Sib_1\,genotype)}{p(Sib_2 genotype)}$$

$$= \frac{\sum_{i=1}^{9}\left(\frac{p(Sib_2\,genotype \cap parental\ comb.i)}{p(parental\ comb.i)}\right)p(parental\ comb.i|\ Sib_1\ \ genotype)}{p(Sib_2 genotype)}$$

Relative Risk for Sibling Carrying a Specific Genotype

For example, the relative risk of *Sib_2Aa*, carrying one copy of the disease allele 'a', is provided by information from the *Sib_1aa* genotype:

$$\Gamma_{Aa|Sib_1aa} = \frac{p(Sib_2Aa|Sib_1aa)}{p(Sib_2Aa)}$$

$$= \frac{½p^2 + pq}{2pq}$$

$$= \frac{½p + (1-p)}{2(1-p)}$$

$$= \frac{1 - ½p}{2 - 2p}$$

Conclusion

- PHI sharing mechanisms are quickly emerging and once in place, they can be used in concert with clinical medical records to achieve a wide variety of innovative health promotion and surveillance goals.
- There are associated ethical and social risks that must be monitored effectively, and privacy decision-making and security for these documents must be improved for adoption to be safe and useful.

Acknowledgements

Committee:
Kenneth Mandl
Peter Szolovits
Isaac Kohane

CHIP Collaborators:
John Brownstein
Karen Olson
Shannon Wieland
IHL Lab

John Tsitsiklis
David Altshuler
Brian Schmidt
John Cloutier
Karin Iancu

HST Students
BIG Students
Friends & Family

Publications Cited

- Cassa CA, Schmidt BW, Kohane IS, Mandl KD. My sister's keeper?: genomic research and the identifiability of siblings. **BMC Med. Gen.** 2008
- Cassa CA, Grannis SJ, Overhage M, Mandl KD. A context-sensitive approach to anonymizing spatial surveillance data: impact on outbreak detection. **J Am Med Inform Assoc** 2006
- Wieland SC, Cassa CA, Berger B, Mandl KD. Revealing the spatial distribution of a disease while preserving privacy. **PNAS 2008** [In Review]
- Cassa CA, Iancu K, Olson KL, Mandl KD. A software tool for creating simulated outbreaks to benchmark surveillance systems. **BMC Med Inform Decis Mak.** 2005
- Cassa CA, Wieland SC, Mandl KD. Re-identification of home addresses from spatial locations anonymized by Gaussian skew. **Int J Health Geogr.** 2008
- Brownstein JS, Cassa CA, Mandl KD. No place to hide--reverse identification of patients from published maps. **N Engl J Med.** 2006
- Brownstein JS, Cassa CA, Kohane IS, Mandl KD. An unsupervised classification method for inferring original case locations from low-resolution disease maps. **Int J Health Geogr.** 2006

Children's Hospital Boston
Informatics Program
Harvard-MIT Division of
Health Sciences and Technology

Geospatial Technology Vis-À-Vis Spatial Confidentiality

Michael Leitner, Ph.D., Associate Professor, Louisiana State University

Abstract:

A common concern when working with health-related data is that national standard guidelines are designed to preserve individual statistical information, usually recorded as text or in a spreadsheet format ('statistical confidentiality'), but lack appropriate rules for visualizing this information on maps ('spatial confidentiality'). Privacy rules to protect spatial confidentiality become more and more important, as governmental agencies increasingly incorporate Geographic Information Systems (GIS) as a tool for collecting, storing, analyzing, and disseminating spatial information.

First, this presentation evaluates the degree to which reverse address-matching or reengineering (i.e., geospatial techniques that include scanning, geo-rectifying, and digitizing) would allow to recover personal data attached to the location of somebody's residence from a map. Preliminary research results demonstrate that only after a few hours of instruction, novices to geospatial technology possess sufficient knowledge to perform successful reverse address-matching. In a second, more applied example, the risk associated with the disclosure of confidential spatial information is investigated using point mortality locations from Hurricane Katrina reengineered from a map published in the Baton Rouge Advocate newspaper.

The second part of this presentation proposes a simple and general framework for presenting the location of confidential point data on maps using empirical perceptual research. The overall objective of this research is to identify geographic masking methods that preserve both the confidentiality of individual locations and at the same time the essential visual characteristics of the original point pattern.

Bio:

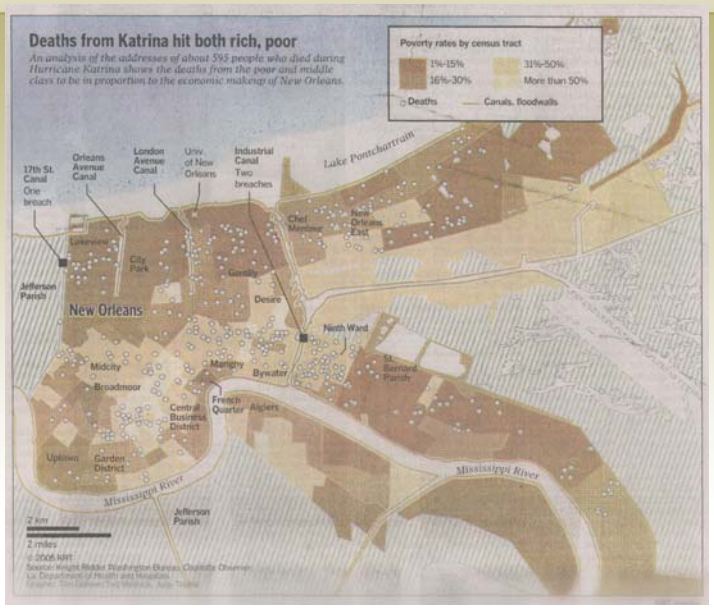
Michael Leitner completed a B.A. (1987) and M.A. (1990) in Geography and Cartography at the University of Vienna, Austria and through a Fulbright Scholarship completed his M.A. in Geographic Information Science (GISc) in 1993 and his Ph.D. in GISc in 1997 in the Department of Geography at the State University of New York. He is currently an Associate Professor (with tenure) in the Department of Geography and Anthropology at Louisiana State University (LSU) in Baton Rouge. Dr Leitner's main research interests are in cartographic generalization and cartographic visualization, as well as, in the research and application of GISc to public safety and public health. He was recently appointed editor of *Cartography and Geographic Information Science (CaGIS)*.

Geospatial Technology Vis-À-Vis Spatial Confidentiality

Electronic Health Information & Privacy Conference
November 3, 2008
Ottawa, Canada

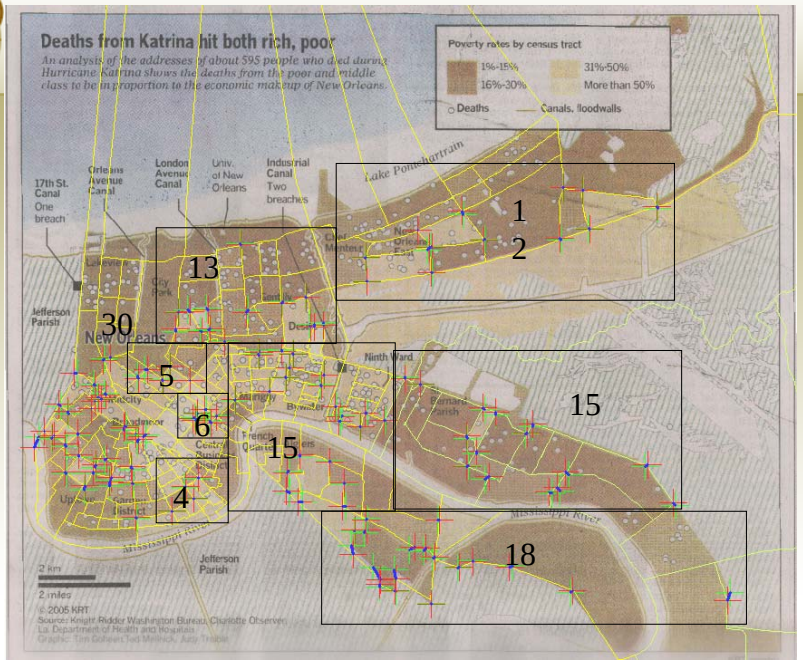
Michael Leitner
Department of Geography and Anthropology
Louisiana State University

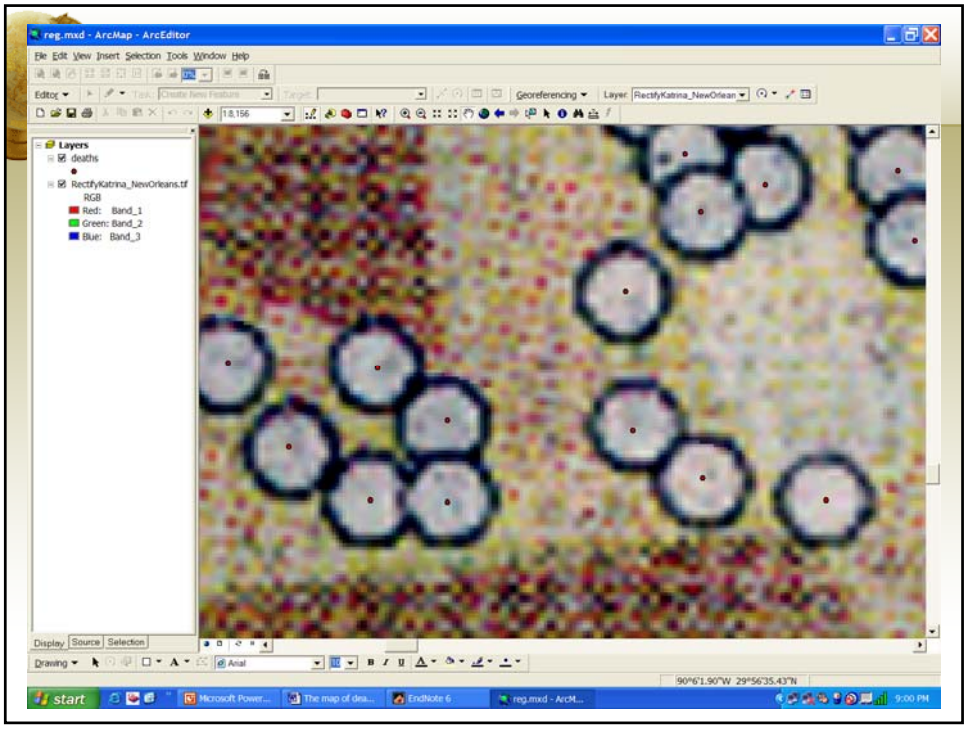
Baton Rouge Advocate, Dec 30th 2005



Reverse Address-Matching

- Scanning
- Geo-rectifying
- Enlarging and digitizing
- Calculating the centroid
- Identifying street address of centroid




reg.mxd - ArcMap - ArcEditor
File Edit View Insert Selection Tools Window Help
Layers
deaths
RectifyKatrina_NewOrleans.tif
RGB
Red: Band_1
Green: Band_2
Blue: Band_3
Display Source Selection
start


CATF4 OUTSIDE
9-9
9/19

New Orleans East

24 mapped deaths re-engineered (red)

16 mapped deaths found (yellow)

London Avenue Canal

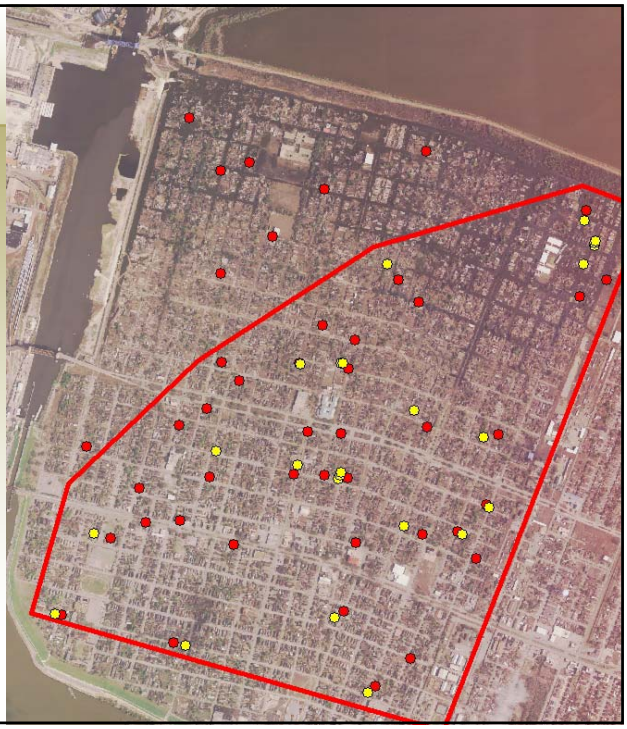
20 mapped deaths re-engineered (red)

14 mapped deaths found (yellow)

Lower 9th Ward

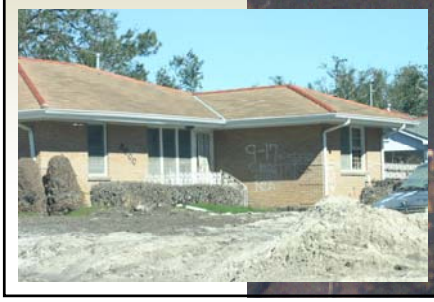
36 mapped deaths
re-engineered (red)

22 mapped deaths
found (yellow)



Detail
New Orleans East

Detail
London Canal



Detail
Lower 9th Ward

Number of Identified Mortality Locations

- New Orleans East: 16 out of 24 (66.67%)
- London Canal Area:14 out of 20 (70.00%)
- Lower Ninth Ward: 22 out of 36 (61.11%)

Research Questions

- How quickly can novices to geospatial technology learn how to re-engineer residential addresses from a map?
- What is the accuracy of such re-engineered addresses?
- Is the accuracy dependent on scale or symbol size?
- What is the relationship between re-engineering and spatial confidentiality?

Reverse Address-Matching and Spatial Confidentiality

- Are fairly new concepts in GISc
- Spatial confidentiality = confidentiality associated with the location of somebody's residence
- Preservation of spatial confidentiality is guaranteed by the citizen's right to privacy

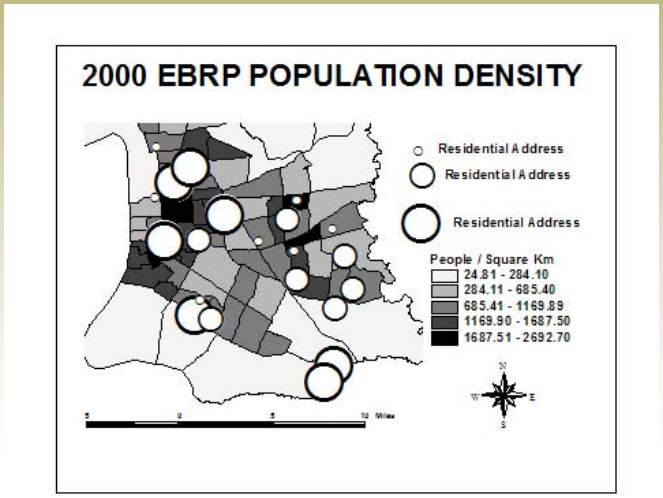
Experimental Design

- 21 test subjects
- Experiment was carried out in an "Introductory GIS" class
- Experiment took place during summer term 2006
- Four students had previously taken a GIS class, seventeen had not
- 19 out of 21 were not originally from Baton Rouge, LA
- Students ranged from 21 to 41 with an average age of 27.2 years
- Participants came from 11 different departments at LSU (3 from geography)
- 10 female and 11 male participants

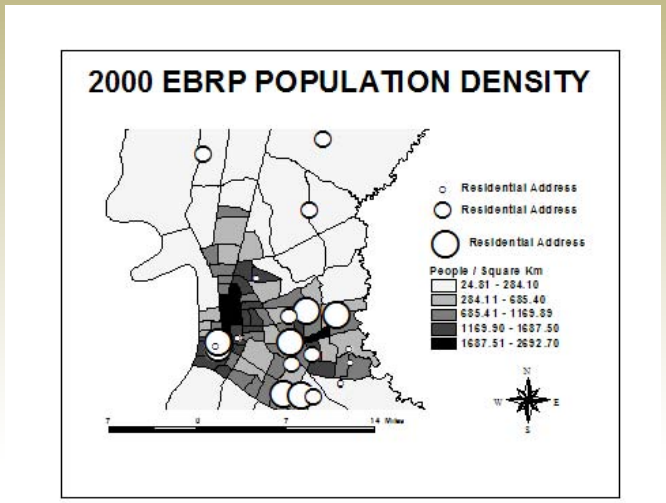
Experimental Design

- Each participant received one test map
- Each test map included 21 residential addresses
- Symbol sizes: small, medium, large
- Map scales: 1:130,000; 1:190,000 and 1:300,000

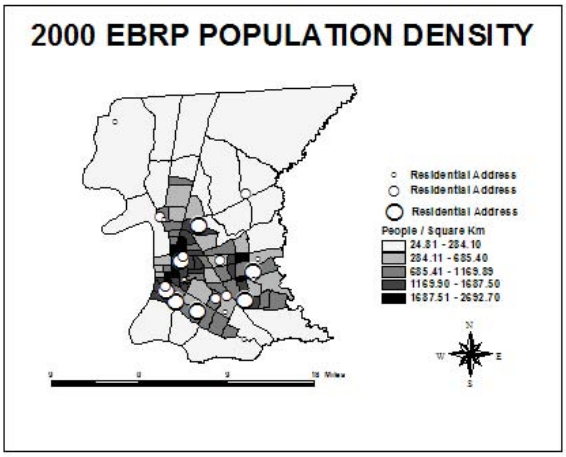
Test Map – 1:130,000



Test Map – 1:190,000



Test Map – 1:300,000



Total Number of Residential Addresses

		Map Scale			
		1:130,000	1:190,000	1:300,000	**Total**
Circle Size	Small	49	49	49	**147**
	Medium	49	49	49	**147**
	Large	49	49	49	**147**
	Total	**147**	**147**	**147**	**441**

Experimental Task – Lab Portion

- Scanning the original test map
- Geo-rectifying to base map
- Heads-up digitizing
- Computing centroids
- Adding U.S. Census street network
- Identifying actual street address closest to each centroid location

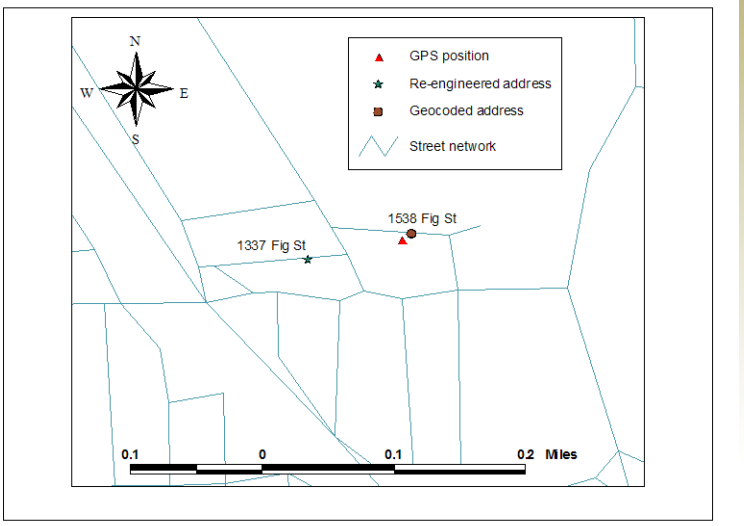
Experimental Task – Field Portion

- Visiting all re-engineered address locations
- Identifying the closest actual street address
- Writing a 1-2 page project report

Capturing Residential Address Locations

- Global Positioning System ("true" location)
- Address-matching
- Inverse address-matching

Capturing Residential Address Locations



Address-Matching and Re-Engineering Errors

- **Address-matching error**
  Distance Between Address-Matched and GPS Position
- **Re-engineering error (1)**
  Distance Between Re-engineered and Address-Matched Position
- **Re-engineering error (2)**
  Distance Between Re-engineered and GPS Position

Research Questions – Answers

- Relative novices to geospatial technology can successfully re-engineer point locations from a map after just a few hours of instructions
- Address-matching error: 1 to 472m (median 42m)
- Re-engineering error (1): 0 to 2089m (median 66m)
- Re-engineering error (2): 8 to 2330m (median 100m)

Influence of Scale

Address-Matching Error[1]	Re-engineering Error (1)[2]	Re-engineering Error (2)[3]	**Scale**
39m	67m	104m	**1:300,000**
45m	65m	101m	**1:190,000**
38m	66m	95m	**1:130,000**

[1]Median Distance Between Address-Matched and GPS Position
[2]Median Distance Between Address-Matched and Re-engineered Position
[3]Median Distance Between Re-engineered and GPS Position

Influence of Symbol Size

Address-Matching Error[1]	Re-engineering Error (1)[2]	Re-engineering Error (2)[3]	**Symbol Size**
52m	44m	88m	**Small**
30m	69m	95m	**Medium**
44m	77m	115m	**Large**

[1]Median Distance Between Address-Matched and GPS Position
[2]Median Distance Between Address-Matched and Re-engineered Position
[3]Median Distance Between Re-engineered and GPS Position

Can Reverse Address-Matching Violate Spatial Confidentiality?

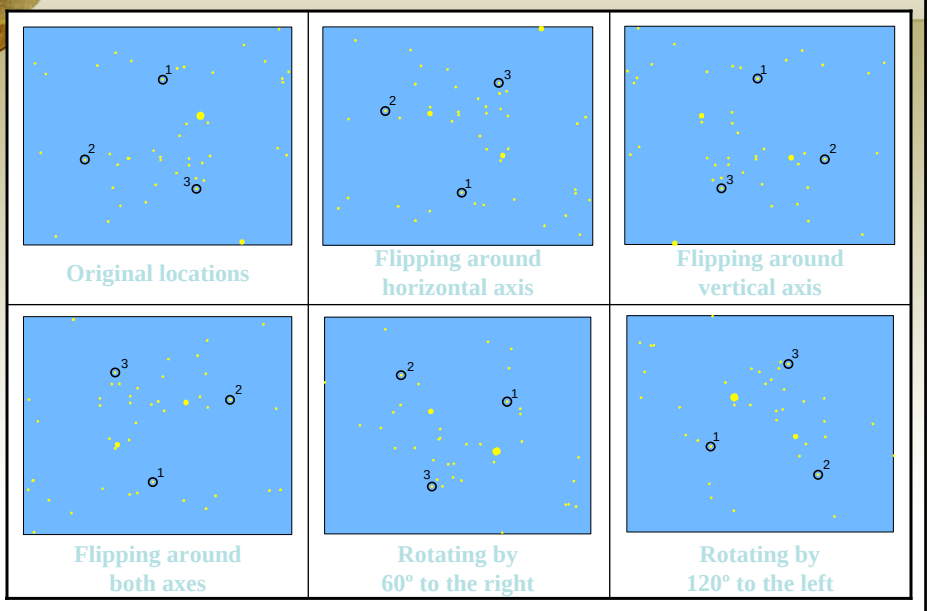
This depends on

- Re-engineering error
- Urban, suburban, rural
- Type of neighborhood (single-family homes, apartment complexes)
- If additional information about residences is available

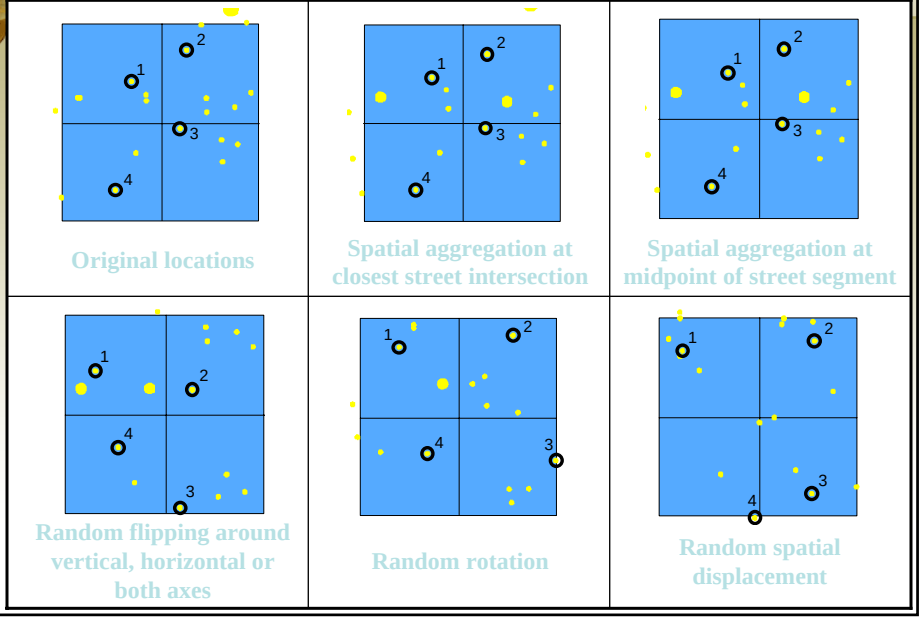
Solution? – Geographic Masking

- Geographic masking slightly modifies the geographic coordinates of the original data points
- Global Geographic Masking
- Local Geographic Masking

Selected Global Geographic Masking Methods



Selected Local Geographic Masking Methods



Geographic Masking

Two types of research areas

- Influencing the visual display of point patterns
- Influencing the results of spatial analysis

How Much Masking is Necessary?

Too much masking

- Changes the visual display of the point pattern
- Biases the results of spatial analysis

Too little masking

- Not preserving spatial confidentiality

Threshold Value for Geographic Masking?

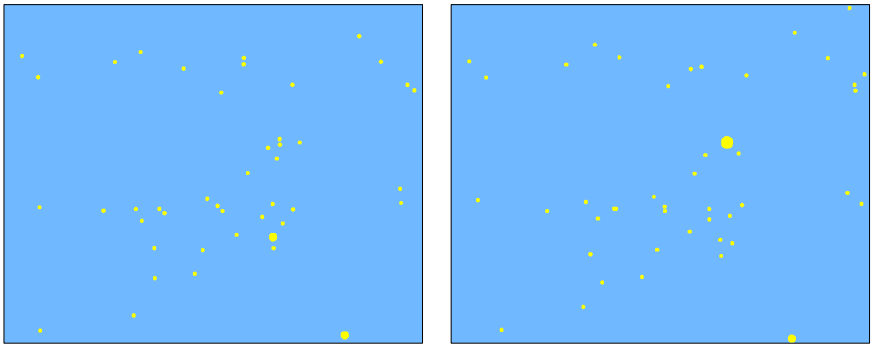
Leitner and Curtis (2006)

- Somewhere between a cell size of 200x200m and 350x350m (40,000 to 122,500m^2)

Kwan *et al.* (2004)

- About the area of a circle with a radius of 279m (244,545m^2)

1st COMPARISON



1. Compare the two point patterns and choose a whole number **between 1 and 7** (1 being VERY SIMILAR and 7 being VERY DIFFERENT): _____

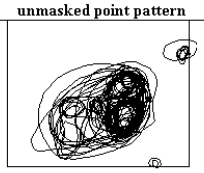
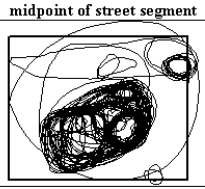
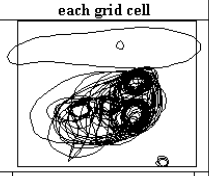
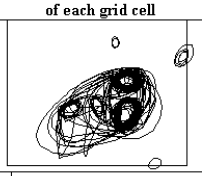
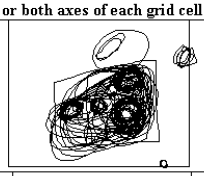
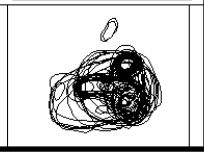
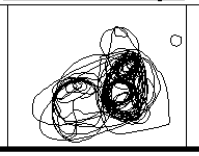
2. In the **LEFT MAP**, identify areas with a high concentration of points or incidents. Mark those areas, if they exist, with a pen or pencil directly on the hard copy map provided.

Similarity Between Original and Masked Point Patterns

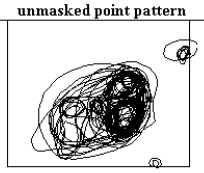
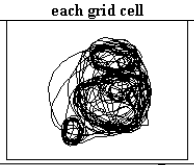
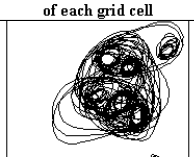
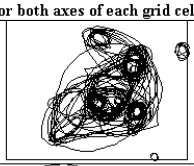
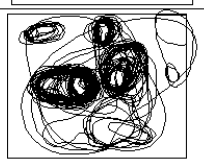
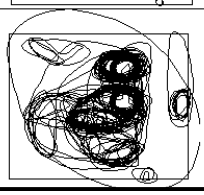
Cell Size	Translating by some random distance within each grid cell	Rotating by some random degree around the center of each grid cell	Flipping randomly either about the vertical, horizontal or both axes of each grid cell
500x500m	4.99	3.64	4.34
350x350m	5.08	4.08	4.20
200x200m	3.60	3.08	3.25
100x100m	3.01	2.77	2.94
	Spatial aggregation at midpoint of street segment	**Spatial aggregation at street intersection**	
	1.80	2.43	

Note: **1 = both point patterns are very similar (little geographic masking)**
7 = both point patterns are very different (much geographic masking)

Perceived Hot Spots

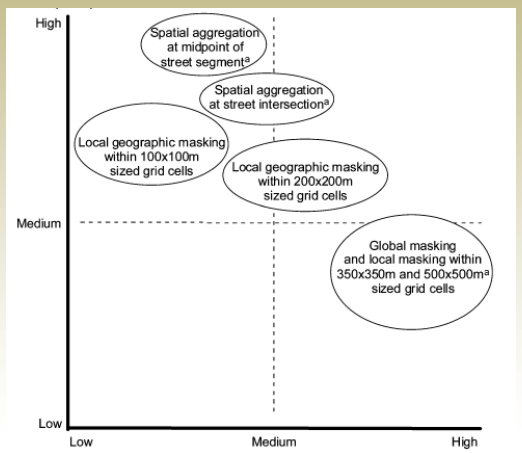
	Original, geographically unmasked point pattern	Spatial aggregation at midpoint of street segment	Spatial aggregation at street intersection
			
Cell size	Translating by some random distance within each grid cell	Rotating by some random degree around the center of each grid cell	Flipping randomly either about the vertical, horizontal or both axes of each grid cell
100x100m			
200x200m			

Perceived Hot Spots

	Original, geographically unmasked point pattern	Spatial aggregation at midpoint of street segment	Spatial aggregation at street intersection
			
Cell size	Translating by some random distance within each grid cell	Rotating by some random degree around the center of each grid cell	Flipping randomly either about the vertical, horizontal or both axes of each grid cell
350x350m			
500x500m			

Relationship Between Amount of Geographic Masking and Preserving Spatial Confidentiality

Similarity between Original and Masked Point Patterns



Preserving Spatial Confidentiality

Problem

National Standards are lacking appropriate guidelines

for visualizing confidential information

Examples

U.S. Department of Health and Human Service (HIPPA)

- " 20,000 people" rule

U.S. Census Bureau

- Areal unit with at least five businesses

U.S. Department of Justice

- No National Standard
- Visualizing confidential information is dependent on departmental policy, state law, Freedom of Information Act, etc.

Discussion

- Points that display personal confidential information should be geographically masked before publishing in a map

Masking methods should be

- Spatially adaptive
- Dependent on the type of data

Alternative methods

- Secure environments
- Software agents (Boulos, et al. 2006)

Thank you for your attention!

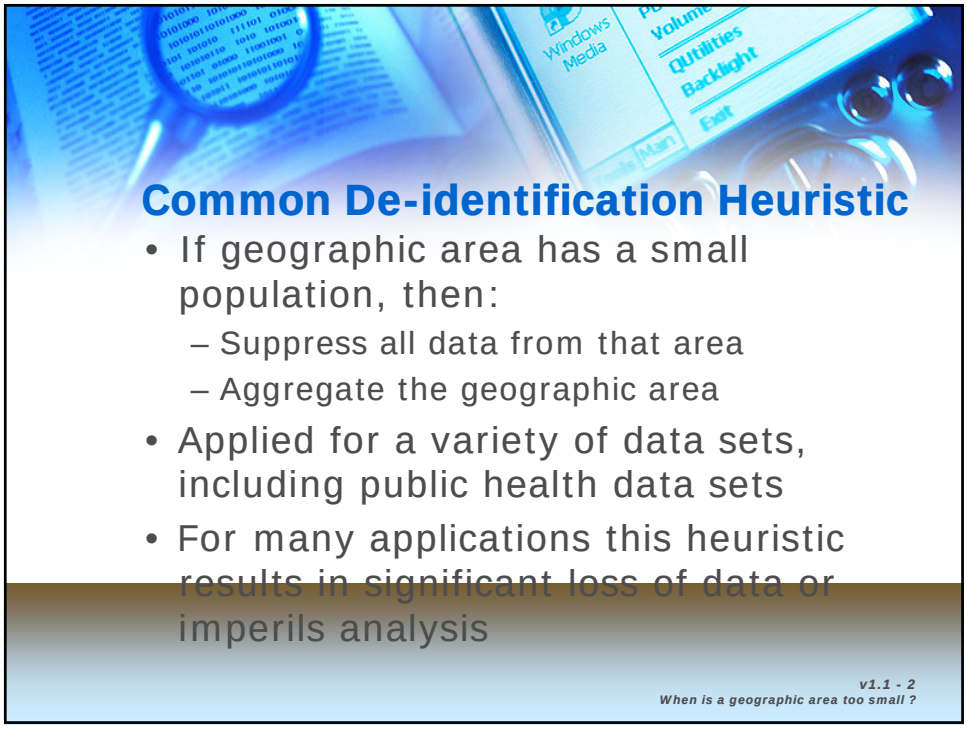
When is a Geographic Area Too Small?

Khaled El Emam, University of Ottawa

Bio:

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/.


When is a geographic area too small ?
Khaled El Emam, University of Ottawa
Ann Brown, CHEO RI
Philip AbdelMalik, PHAC


Common De-identification Heuristic
• If geographic area has a small population, then:
– Suppress all data from that area
– Aggregate the geographic area
• Applied for a variety of data sets, including public health data sets
• For many applications this heuristic results in significant loss of data or imperils analysis
v1.1 - 2
When is a geographic area too small ?

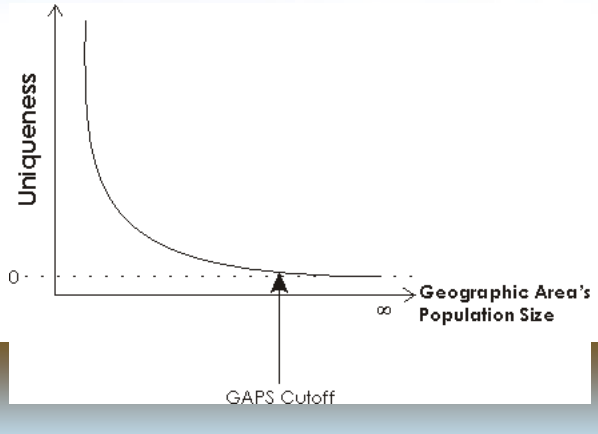
Examples

- HIPAA: 20k rule
- Census Bureau: 100k rule
- Statistics Canada: 70k rule
- British Census: 120k rule

The Problem

- Such generic rules ignore the specific variables that are included in a data set
- A smaller cutoff should be used if few variables are in a data set
- A larger cutoff should be used if many variables are in a data set

Empirical Observation



Our Analysis

- We performed a simulation analysis of regions using Canadian 2001 Census data to empirically determine the cutoffs
  - The number of variables were varied
  - The region size was varied
- Based on that we developed a model to predict the cutoffs – the point at which the uniqueness plateaus

Application of Results

- We applied our models to the problem of prescription data that is sold by retail pharmacies to data analysis companies
- The question was whether patients can be re-identified from these prescription records
- The variables that are relevant: age, gender, and FSA

Province	Our GAPS Models		20,000 Cutoff		70,000 Cutoff		100,000 Cutoff	
	FSA	Pop	FSA	Pop	FSA	Pop	FSA	Pop
Alberta	55%	84%	38%	71%	1.4%	5%	0	0
British Columbia	68%	87%	46%	70%	1.1%	4%	0	0
Manitoba	59%	88%	39%	68%	0	0	0	0
New Brunswick	20%	51%	4.5%	19%	0	0	0	0
Newfoundland	55%	83%	30%	62%	0	0	0	0
Nova Scotia	47%	82%	16%	43%	0	0	0	0
Ontario	69%	91%	49%	76%	1.4%	5%	0.2%	1%
PEI	57%	90%	43%	79%	0	0	0	0
Quebec	59%	84%	36%	63%	1%	5%	0.25%	0.1%

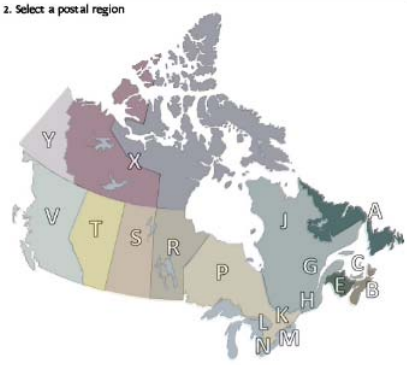
Automation - I

Region

1. Enter the maximum number of combinations for the variables

172

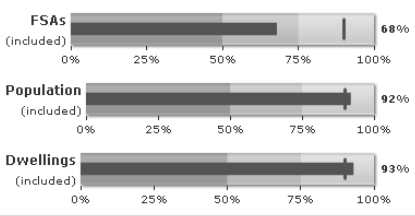
2. Select a postal region



Automation - II

FSA	Population	Dwellings
K7P	13749	4781
K7R	13911	5964
K7H	14371	7247
K2P	14820	10240
K7C	15125	6165
K2A	15379	6887
K1H	15933	6999
K2M	16304	5291
K2K	16460	5612
K2S	16513	5528
K7A	16626	6748
K1E	16907	5461
K6J	17470	7742
K1L	18258	9340
K1B	18662	6574
K1R	19061	10379
K2E	19078	7671

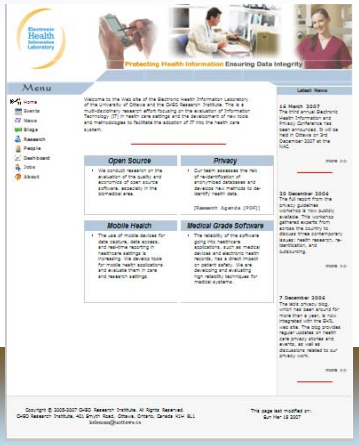
This shows the proportion of the population and dwellings in the Postal Region="k" that are considered to have acceptable re-identification risk according to this cutoff criterion.



Acknowledgements

- This work was funded by:
  - GeoConnections (Natural Resources Canada)
  - Ontario Centers of Excellence
  - Public Health Agency of Canada

www.ehealthinformation.ca



Session 2B: Privacy Law

Session Chair: Murray Long, Privacy Consultant and Founder of Murray Long & Associates Inc.

Bio of Chair:

Murray Long is a leading Canadian privacy consultant.

He was a member of the Canadian Standards Association (CSA) Privacy Committee that drafted the Model Code that is built into Canada's new private sector privacy law. He was also the principal author of *How to Make the CSA Code Work for You*, a workbook published by the CSA that explained in detail how to apply the Code.

In 1997, after establishing his own consulting practice, he provided consulting services to Industry Canada on new privacy legislation. With the tabling of PIPEDA in Parliament in October 1998, he established an electronic newsletter called **PrivacyScan** that continues to provide timely and useful information on privacy issues in Canada. With the passage of PIPEDA, he has provided guidance on compliance to organizations in the telecommunications, financial, transportation, retail, franchising, health and charitable sectors as well as government agencies, law firms and advocacy groups.

Mr. Long writes and speaks extensively about privacy law. Since 2002, he has presented workshops on privacy law implementation across Canada for the CSA. He has developed privacy training courses in collaboration with Sask Tel, the Office of the Privacy Commissioner and the Canadian Payroll Association, and was the author of a CD ROM-based privacy training tool for the CSA. Along with Suzanne Morin, a senior lawyer at Bell Canada, Murray was co-author of the **Canadian Privacy Law Handbook**, the first annotated guide to the new law, published in June, 2000. More recently, he authored a book on payroll privacy published by the Canadian Privacy Association. He is currently writing a new annotation of PIPEDA.

Re-identification in the Canadian Adverse Drug Reaction Information System: The Gordon Case

Ross Hodgins, Office of the Information Commissioner

Abstract:

The Federal Court case involving the Canadian Adverse Drug Reaction Information System (CADRIS) is a notable example of the challenge of balancing the principles of providing access to information and protecting the privacy of individuals. CADRIS is a database comprised of over 40 years of records, each with up to 130 fields of data about individuals who have suffered adverse drug reactions. While the majority of fields can be disclosed in response to access requests, 12 fields must be withheld on the basis that they are either explicit identifiers or their disclosure would permit re-identification. Health Canada had sought the assistance of statistical experts to determine the degree of vulnerability of the various fields to re-identification and to help develop a methodology to facilitate the decision-making process for CADRIS and similar databases.
The requester sought redress in Federal Court regarding the Department's refusal to disclose the field of "province". In a landmark decision in favour of Health Canada, the Court clarified the definition of personal information in the *Privacy Act* as "information about an identifiable individual where there is a serious possibility that an individual could be identified through the use of the information, alone or in combination with other available information."

Bio:

In June 2008 Ross Hodgins began working at the Office of the Information Commissioner. He provides advice regarding policy and systemic issues in the field of access to information.

Prior to working in the Commissioner’s Office, Ross was the Director of the Access to Information and Privacy Division in Health Canada. He was responsible for establishing a centre of privacy expertise within the Department and for collaborating with representatives from the health sector to advance the protection of personal health information. In addition, he managed the operational unit that responded to access to information and privacy requests.

For many years, Ross was a Senior Advisor at the Treasury Board Secretariat. During his career at the Secretariat he developed several information management, communication, access to information and privacy policies. In the privacy field, he implemented government-wide policies and guidelines related to data matching, control of the Social Insurance Number and privacy impact assessments.

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

De-Identification / Re-identification

Canadian Broadcasting Corporation
v. Minister of Health

Electronic Health Information and Privacy Conference
November 3, 2008

CADRIS

(Canadian Adverse Drug Reaction Information System)

- Program responsible for collecting and assessing adverse reaction reports related to pharmaceuticals, biologics and natural health products
- Database comprised of suspected adverse reactions reported by
  - health professionals and laypersons (38%) – voluntary
  - manufacturers (62%) – mandatory
- Over 40 years of records, each with up to 130 fields of data
- One of several Health Canada databases subject to routine access to information requests

Issue

- Health Canada exempted 12 of 130 data fields as personal information
- Fields included explicit personal identifiers and fields that, when combined with others, could render an individual identifiable, including
  - patient initials
  - patient identification number
  - date of conception / birth / death
  - notifier clinic / hospital / telephone number
  - notifier province

Information Commissioner's Investigation

- Health Canada's position regarding its refusal to disclose 12 fields
  - permit re-identification – risks verified by Statistics Canada
  - majority of fields already disclosed – no "greater public interest" served
  - "chilling" effect on voluntary sources resulting in less information being available
- CBC's position
  - not all 12 fields qualify as personal information
- Information Commissioner
  - recommended 3 fields be coarsened from "date of" to "year of" – conception / birth / death
  - complaint not well-founded

Insider Intruder Test

- Methodology relies on probability that the person conducting the search has information about the subject
- Example
  - If a neighbour is known to have died as the result of an adverse drug reaction, a search can be conducted with known information, e.g. gender, age, date of death, approximate height and weight, city and province
  - If the results of the search provide a small number of reports or a single report, the neighbour can be identified with a high degree of probability
  - More than 100 additional fields of potentially sensitive health data become available, e.g. HIV medication or stay at a psychiatric hospital

Example 1

Parameters of Search	Number of Reports
Notifier Province: Alberta	1462
Notifier City: Edmonton	550
Reason for Serious: Death	31
Patient Age: Patient 50-60 years of age	5

Parameters of Search	Number of Reports
Notifier Province:	Not Searched
Notifier City:	Not Searched
Reason for Serious: Death	8075
Patient Age: Patient 50-60 years of age	1322

Report Id	Date Received	Type of Notifier	Age	Gender	Reason for Serious	City	Clinic (Address)	Hospital
135616	2000-11-23	Physician	56	M	Death	Edmonton	15508-87 Ave NW	-
136249	2000-12-27	Health professional	53	M	Death	Edmonton	-	Alberta Hospital
137518	2001-03-06	Physician	56	M	Death	Edmonton	15508-87 Ave	-
165509	2003-11-05	Physician, specialized	57	F	Death	Edmonton	34rd Fl, 9942-108 St	Dept of Psychiatry, U of A
174457	2004-09-13	Physician, specialized	52	M	Death	Edmonton	Bldg 31-8770 165 St	-

Example 2

Parameters of Search	Number of Reports
Notifier Province: Prince Edward Island	681
Notifier City: Charlottetown	189
Patient Age: Patient 50-80 years of age	46
Patient Gender: Male	11
Reason for Serious: Caused Prolonged Hospitilization	2

Parameters of Search	Number of Reports
Notifier Province: Prince Edward Island	681
Notifier City:	Not Searched
Patient Age: Patient 50-80 years of age	209
Patient Gender: Male	79
Reason for Seriousness: Caused Prolonged Hospitilization	11

Report Id	Date Received	Type of Notifier	Age	Gender	Reason for Serious	Province	City
24708	1980-06-25	-	58	M	Caused Prolonged Hospitilization	Prince Edward Island	Charlottetown
80491	1992-04-09	-	56	M	Caused Prolonged Hospitilization	Prince Edward Island	Charlottetown

Example 3

Parameters of Search	Number of Reports
Gender: F	101079
***Age:** 30-40 years old	13738
Province: New Brunswick	1095
Ethnicity: African	1

Report Id	Date Received	Gender	Age	Province	Ethnicity
154035	1993-06-14	F	33	New Brunswick	African

Catherina's Story

- CBC News – "Did Catherina's use of Diane-35 contribute to the young woman's death?"
- Diane-35 used for acne and birth control
- Reporter used information from CADRIS and an obituary database
- Reporter identified and contacted Catherina's family

Mike Gordon and The Minister of Health and The Privacy Commissioner of Canada, CFN: T-347-06, February 4, 2008

- Health Canada
  - refused access to "province" field in CADRIS database
  - exempted as personal information
- CBC
  - province not personal information – identification requires speculation
  - Health Canada failed to exercise discretion to disclose the information in the "public interest"
- Privacy Commissioner
  - personal information is "information about an identifiable individual where there is a serious possibility that an individual could be identified through the use of the information, alone or in combination with other available information"

Federal Court Decision February 27, 2008

- CBC's application was dismissed
- Supported the "serious possibility" test put forward by the Office of the Privacy Commissioner
- Upheld Health Canada's exercise of discretion not to disclose information in the "public interest" as a "conclusion he [the head of the institution] was entitled to make" (*Dagg v. The Department of Finance*)
- Confirmed the relevance of the current risk based approach

Lessons

- CADRIS database mounted on Health Canada's website
- Recognition that re-identification may be accomplished without intervention of experts
- Expertise in the field of de-identification / re-identification increasing
- Policy and guidelines on de-identification / re-identification being developed to assist program and database managers

Policy and Guidelines

- Core elements
  - Guidance for decision making
  - Assessing information sensitivity
  - De-identification methodologies
  - Quantification of re-identification and risks assessment solution
  - Mandatory provisions for controlled releases
  - Standards
  - Contracting out requirements
- Strategies
  - Data release monitoring
  - Data de-identification committee

Nothing Personal

- Privacy protection in support of health policy objectives
- Systematic approach to manage privacy and re-identification risks
- Applicability to other programs, e.g. Canadian Hospitals Injury Reporting and Prevention Program (CHIRPP)
- Information Commissioner's *Annual Report to Parliament: 2007-2008*

  Health Canada's performance on the CHIRPP case was an "innovative way to resolve a complaint" and an "excellent example of a federal institution providing every assistance to a requester."

Ross Hodgins

Senior Advisor
Policy and Systemic Issues
Office of the Information Commissioner of Canada
613-943-4369
rhodgins@infocom.gc.ca

PHIPA Review: Prescription for the Future

Carol Appathurai, Director of PHIPA Review Project, Minstry of Health and Long-Term Care.

Bio:

Carol Appathurai is a Director in the Ministry of Health and Long-Term Care. Carol had responsibility for the development of Ontario's *Personal Health Information Protection Act* in 2004 and is now leading the legislatively mandated review of the Act. She has had a long involvement in strategic policy development in Ontario's Ministry of Health and Long-Term Care and Ministry of Community and Social Services, and, at the federal level, in Health Canada. She has a B.A. and an M.A. from the University of Toronto.

EHIP Conference

Personal Health Information Protection Act, 2004 (PHIPA) Review

Carol Appathurai
Health System Strategy Division

Ontario

PHIPA Review Process

- The *Personal Health Information Protection Act, 2004* (PHIPA) came into force on November 1, 2004 and establishes rules for the collection, use and disclosure of personal health information in Ontario
- Section 75 requires that a "comprehensive review" be initiated by a Committee of the Legislature within three years of its coming into force
- Within one year from the beginning of the review, the Legislative Committee must make recommendations to the Legislative Assembly concerning amendments to PHIPA
- The Committee held a public Hearing on the review on August 28, 2008

Ontario

Recommendations from Stakeholders
3

❖Education

- More precise definition, clarification e.g. “circle of care”
- Education on rights and responsibilities for custodians and the public
- Customized materials for mental health and others with special needs
- Create user-friendly access to information

Ontario

Recommendations from Stakeholders
4

❖Fees

- Prescribe fee guidelines
- Ensure fees for access to personal health information are as low as possible with mechanisms for exempting low-income individuals from charges
- “Reasonable cost recovery” should not be interpreted as nominal payment
- Streamline the complaints and appeals mechanism on fees with a 7 day mandatory response time and reasons
- Waive direct site access fees

Ontario

5

Recommendations from Stakeholders

❖**Disclosure without consent of personal health information to family members of adult mental health patients**

- Allow families to obtain access to the health information of mental health patients without consent (make part of circle of care or follow B.C. continuity of care purpose)
- Treat mental health information as "special type" of information to allow for collection of collateral information for mental health patients without consent
- Allow family members to disclose personal information to health information custodians and protect the identities of those who provide second-hand information to health information custodians

Ontario

6

Recommendations from Stakeholders

❖**Breaches**

- Make breach notification consistent with that proposed for PIPEDA
- Provide more direction on what types of breach situations should be reported to patients
- Mandatory notification to IPC should be reserved for limited circumstances, where warranted by degree of harm

Ontario

7

Recommendations from Stakeholders

❖Privacy Impact Assessments (PIAs)

- Mandatory PIAs but only in limited and prescribed circumstances, such as when multiple organizations are involved
- Provide greater clarity respecting the components of a PIA and when they should be conducted
- Provide more direct access to tools, templates and expertise

Ontario

8

Moving Forward

Secondary Uses: Individual Right to Privacy vs. the Public Good

- With large scale data banks comes increased demand for a wider ranges of uses, more ample and accelerated circulation of phi to more end users
- Risks:
  - Technology-driven triangulation of data
  - Vulnerable populations
  - Pressure from police and immigration services to gain access (UK). In the USA:

    The proposed national health information infrastructure will yield many other benefits in terms of new opportunities for access to care, care delivery, public health, ***homeland security,*** *and clinical and health research" (Institute of Medicine, 2004)*

Ontario

9

Moving Forward

- **New Technologies: Individual right to privacy vs. benefits of new technologies**
- **Portable computing**: wireless laptops, PDs, Blackberries, DVDs, memory drives – ability to carry full patient histories and clinical files
- **Patient Portals: allows patients to login over the Internet and**
  - update or modify their records
  - dialogue with physicians
  - view prescriptions
  - refill prescriptions
  - View lab-tests requests
- **Radio Frequency Identification Devices (RFID**

Ontario

10

Moving Forward

Genetic Information

- Genetic information is:
  - fundamentally personal and sensitive.
  - Not just information about the person tested, but that person's parents, siblings and offspring –complicates the right of privacy
  - Amount of information obtainable from a DNA sample, the longevity of the sample and the possibility of re-testing and discovery of new uses.
- Many non-medical uses of this information carry negative implications:
  - Insurers can use it to deny health or life insurance
  - Employers can use it to exclude hiring people less than genetically perfect but healthy
  - Banks can used it to determine who gets a mortgage
  - Schools can use it to stream children into particular programs
  - Social implications

Ontario

Privacy in Healthcare: Just good business

- Often argued that incorporating privacy into organizational practice too costly and onerous
- Privacy helps to achieve strategic goal of effective healthcare by strengthening the trust relationship between the individual and the organization
- Trust relationship fosters meaningful (uninhibited) participation and improves outcomes; improves access for vulnerable populations
- In healthcare, trust is dependent on:
  - ability to assure patients that their information is being kept private and secure.
  - No surprises – transparency of information collection, use and disclosure practices
- How can healthcare providers be educated on value of investing in privacy protections

Ontario

When is Location Data “Personal Information”?

Teresa Scassa, Canada Research Chair in Information Law, Faculty of Law, University of Ottawa

Abstract:

Data protection legislation typically protects data that is “personal information about an identifiable individual”. Location data can become personal information, where, in combination with other data, it becomes data about an identifiable individual. Yet the boundaries of these concepts are not always clear. This presentation will explore the meaning of “personal information” in relation to location data through a consideration of Canadian case law on the issue.

Bio:

Teresa Scassa holds undergraduate law degrees in civil and common law from McGill University, as well as an LL.M. and an S.J.D. from the University of Michigan. She is Canada Research Chair in Information Law, at the Faculty of Law, University of Ottawa, Common Law Section. Dr. Scassa is a researcher with a GEOIDE funded research project titled: *Public Protection and Ethical Geospatial Dissemination: Social and Legal Aspects*. Her research focus in this project is on privacy issues. Dr. Scassa is a member of the External Advisory Committee to the Privacy Commissioner of Canada. She has published many articles in a range of areas of law, including intellectual property law, privacy law and law and technology. She is co-author of the book *Electronic Commerce and Internet Law in Canada*.

When is Location Data Personal Information?

Dr. Teresa Scassa
Canada Research Chair in Information Law
University of Ottawa, Faculty of Law

Electronic Health Information and Privacy Conference
November 3, 2008

Why does it matter?

- Data protection regimes in Canada govern the collection, use and disclosure of “personal information” in a variety of contexts
- When location data is considered to be personal information, data protection legislation will apply

Location Data

- Location Data can include any geographic information that can identify the location of a person, place or thing
- Location data may be extremely precise, or it may provide a more general set of co-ordinates

Location Data

- Location data when combined with information about the incidence of disease, prescribing practices, or other health-related information can be extremely valuable in medical research, public health planning, etc.
- But when is location data personal information that is subject to the rules governing the collection, use and disclosure of such information?

Personal Information: Statutory Provisions

- Data protection legislation generally applies to “personal information about an identifiable individual”

Personal Information Protection and Electronic Documents Act (PIPEDA)

- “personal information” means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Alberta

- *Personal Information Protection Act*: "personal information" means information about an identifiable individual

Alberta -- *Health Information Act*

- "individually identifying", when used to describe health information, means that the identity of the individual who is the subject of the information can be readily ascertained from the information;
- "non-identifying", when used to describe health information, means that the identity of the individual who is the subject of the information cannot be readily ascertained from the information;

Alberta -- *Health Information Act*

- 32**(1)** A custodian may disclose non-identifying health information for any purpose.
- **(2)** If a disclosure under subsection (1) is to a person that is not a custodian, the custodian must inform the person that the person must notify the Commissioner of an intention to use the information for data matching before performing the data matching.

Ontario – *Personal Health Information Protection Act* (PHIPA)

- "personal health information" . . . means identifying information about an individual in oral or recorded form,. . .
- "identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

Personal Information: A Two-Part Test?

- Information is personal information if it is ". . . "about" an individual **and** if it permits or leads to the possible identification of the individual. There is judicial authority holding that an "identifiable" individual is considered to be someone whom it is reasonable to expect can be identified from the information in issue when combined with information from sources otherwise available" (*Canada (Information Commissioner v. Canada (Transport Accident Investigation & Safety Board*) (FCA, 2007)

"Identifiable Individual"

- An individual is identifiable if the information "permits or leads to the possible identification of the individual"
- "the individual must be "identifiable", not necessarily *identified*." (PIPEDA Finding #349)

"Identifiable Individual": *Gordon v. Canada* (F.C. 2008)

- Access to Information request for release of information in Canadian Adverse Drug Reactions Information System (CADRIS)
- Data in field "province" was withheld by Minister on the basis that it might allow for the identification of individuals

"Identifiable Individual"

- *Gordon v. Canada (Minister of Health)* (F.C. 2008): "information recorded in any form is information "about" a particular individual if it "permits" or "leads" to the possible identification of the individual, whether alone or when combined with information from sources "otherwise available" including sources publicly available."

"Identifiable Individual": *Gordon v. Canada* (F.C. 2008)

- Gibson J. accepted that if released, this information: "would substantially increase the possibility that information about an identifiable individual that is recorded in any form would fall into the hands of persons seeking to use the totality of information disclosed from the CADRIS database, in conjunction with other publicly available information, to identify "particular" individuals."

"Identifiable Individual": *Gordon v. Canada* (F.C. 2008)

- Gibson J. accepts standard proposed by Privacy Commissioner of Canada: "Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."

"Identifiable Individual": *Gordon v. Canada* (F.C. 2008)

- Court heard evidence regarding how information about "province" could increase the possibility of identifying individuals
  - Data could be matched with obituary data available on the internet
  - Other information could be known by a neighbour or hospital worker

"Identifiable Individual"

- Aggregate data about a group of people may be the personal information of members of that group so long as the members are identifiable

(Order F05-14: *British Columbia (Ministry of Public Safety and Solicitor General)(Re)* (2005, B.C.I.P.C.))

"*About*" an identifiable individual

- To be personal information, the information in question must be "**about**" the individual
- Court and privacy commissioner decisions suggest that information linked to an identifiable individual may sometimes be "**about**" something other than that individual

"*About*" an identifiable individual

- Recorded communications between pilots and air traffic controllers is not the personal information of those individuals because it is not **about** them (*Canada (Information Commissioner v. Canada (Transport Accident Investigation & Safety Board)* (FCA, 2007))
- Information was instead "non-personal information transmitted by an individual in job-related circumstances"

"*About*" an identifiable individual

- Copies of building logs with names, ID numbers and signatures of Dept. of Finance employees who signed the sheets when entering and leaving work on weekends is not personal information because it is not *about* the employees, it is about "the position or functions of the individual" (*Dagg v. Canada*, SCC 1997)

"*About*" an identifiable individual

- 2001 Complaint against a U.S. based company that gathered and sold data about physician prescribing patterns
- "the meaning of "personal information", though broad, is not so broad as to encompass all information associated with an individual." (PIPEDA Case Summary #14)

"*About*" an identifiable individual

- "An individual prescription, though potentially revealing about a patient, is not in any meaningful sense *about* the prescribing physician as an individual." (PIPEDA Case Summary #14)
- Such information considered to be "work product"

Other characteristics of "personal information"

- "personal information" may be inferred information (PIPEDA Finding #349)
- "personal information" need not be true or accurate
- A piece of information may be the personal information of more than one individual

Location Data and Personal Information: Concluding Thoughts

- Information about the location of an identifiable individual in general or at a specific point in time is typically personal information
- General location data, when combined with other pieces of information may amount to personal information if it renders specific individuals identifiable

Location Data and Personal Information: Concluding Thoughts

- The degree of identifiability of individuals is described in different terms in different contexts:
  - "permits or leads to" a "possible" identification (*Canada (Inf. Comm'r) v. Canada (Transport Accident Investigation & Safety Board)*)
  - "serious possibility" (*Gordon v. Canada*)
  - Readily ascertainable – (Alberta *Health Information Act)*
  - "reasonable expectation" that the individual can be identified from the information (Orders under ONtarios FIPPA and MFIPPA)

Location Data and Personal Information: Concluding Thoughts

- Does the seriousness of a possibility or the reasonableness an expectation turn on:
  - The ease with which connections can be made
  - The commercial or other value of the information (i.e. the likelihood someone will try to make the connections)
  - The sensitivity of the information (potential for harm to individual if connections made)?

Questions?

Thank You

Session 1C: Secondary Use and Population Registries

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

Bio 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.

The Secondary Use of Electronic Health Records for Health Research Purposes

Patricia Kosseim, Chief GE3LS Officer, Genome Canada

Abstract:

Driven by government priorities and significant financial investments, stakeholders in Canada are working actively to develop and deploy pan-Canadian, interoperable electronic health record (EHR) systems. Efforts to date have concentrated primarily on health care purposes only. However, limiting the design and incremental roll out of such systems for this primary purpose now will only increase the complexity of allowing access to electronic health records for secondary research purposes later.

The likely effect of deferring questions concerning secondary uses will be an exacerbated policy dilemma that drives solutions further away from the well-established norm of voluntary and informed consent as a core component of privacy protection. Kosseim will argue that such a shift – if or when it happens – should not occur without critical reflection, open policy debate, and a democratic decision-making process. In particular, a shift away from consent as a key pillar of privacy protection in the health system must not be motivated solely by technological design and feasibility considerations – issues that arise as an automatic consequence of other, merely pragmatic choices being made today.

In her presentation, Kosseim will discuss policy alternatives that could permit access to EHR data for research purposes. Her aim is to convey why legal and policy considerations require early reflection and up-front integration into systems as they are being designed. By introducing and discussing a range of policy options that address research access to EHR systems, Kosseim endeavors to support informed deliberations about available choices before technological imperatives pre-determine the selection.

Bio:

Patricia Kosseim has recently joined Genome Canada on a two-year Executive Exchange arrangement to develop and implement a national/international strategy for integrating ethical, economic, environmental, legal and social (GE3LS) aspects into large scale genomics research. She joins Genome Canada from the Office of the Privacy Commissioner of Canada (OPC), where she held the position of General Counsel since January 2005, responsible for the activities of the Legal Services, Policy and Parliamentary Affairs Branch. In that capacity, Patricia provided legal and policy advice on complex privacy issues in both public and private sectors; represented OPC before the Federal Courts of Canada and Parliamentary Committees; directed and conducted legal and policy research on the impact of emerging information technologies; and worked collaboratively with stakeholders on legal and policy initiatives across multiple jurisdictions, both nationally and internationally.

Before joining OPC, Patricia spent five years at the Ethics Office of the Canadian Institutes of Health Research leading major initiatives aimed at: developing health policy from an ethical, legal and social perspective; promoting a culture of ethics and integrity in health research; and strengthening Canada's health research capacity in areas of ethics, law and social sciences. During this period, she was briefly seconded to Canada Health Infoway Inc. to advise on privacy 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, professional regulation and civil and commercial litigation.

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, and 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.

Electronic Health Information & Privacy Conference

Ottawa, Ontario
November 3, 2008

Policy Options for Allowing Research Use of E.H.R.s

Presentation By: Patricia Kosseim

Presentation based on:

P. Kosseim and M. Brady,
"Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes", (2008) 2 *McGill Journal of Law and Health* 5

Available online:
http://mjlh.mcgill.ca/texts/volume2/pdf/MJLH_vol2_Kosseim-Brady.pdf

Main Thesis

- To date, efforts and investments aimed at developing and deploying pan-Canadian, interoperable E.H.R. systems have focussed primarily on health care and treatment purposes.

- The design and incremental roll out of E.H.R. systems for this limited purpose *now*, will likely increase the complexity of determining access rights to E.H.R.s for secondary purposes *later*...

Main Thesis

- Deferring questions of 2° uses will likely exacerbate the current policy dilemma by driving solutions away from the default standard of informed consent to accommodate growing pressures for technological expedience, design and feasibility.
- Yet, fundamental public policy choices, we argue, must be based on principle, not merely pragmatism…

Main Thesis

- A shift away from informed consent as the default standard for research – *if or when it happens* - should not occur without critical reflection, open policy debate and a democratic decision-making process.
- To assist policy-makers in that deliberative process, we attempt to explain why informed consent remains the default standard currently at law and then go on to critically analyze six viable policy options for permitting research access to E.H.R. data…

Legal Foundations of Informed Consent as the Default Standard

- Clinical Research
- Epidemiological Research
- Creation of Research Platforms

Legal Foundations of Informed Consent as the Default Standard

In the case of clinical research, informed consent is based on the right to control what shall be done with one's body and to limit undue physical intrusions upon the person.

Legal Foundations of Informed Consent as the Default Standard

In the case of retrospective research involving 2° use of data originally collected for a different purpose, informed consent is based on the right to control what is done with one's personal information and to limit unjustified invasions of one's reasonable expectation of privacy.

Legal Foundations of Informed Consent as the Default Standard

In the case of prospective research using data collected for the purpose of creating a research platform to support future research, informed consent is (arguably) based on the right to exercise autonomy over decisions affecting fundamentally important aspects of one's life.

In view of the growing recognition that informed consent may not always be feasible for all types of health research using E.H.R. data, we consider a broader spectrum of viable policy alternatives together with their implications, which have yet to be more fully explored in an open, transparent and inclusive public policy debate…

Policy Option # 1

Obtaining Informed Consent for Each Specific Research Study

Policy Option # 2

Seeking Broad Consent for Future, Yet Unspecified Research Studies

Policy Option # 3

Using De-Identification as a Means of Carving Out Research Activities Altogether

Policy Option # 4

Relying on Implied Consent by Re-Conceptualizing Research as a Necessary Adjunct to the Primary Purpose of Health Care

Policy Option # 5

Resorting to Existing Statutory Consent Exemptions for Research

Policy Option # 6

Retroactively Deeming Consent by Legislative Amendment

Conclusions

Through this spectrum of options, we have attempted to demonstrate why legal and policy considerations require early reflection and up-front integration into systems as they are being designed, and cannot be so easily retro-fitted after the fact. This critical discussion of various options will hopefully support informed deliberations about available public policy choices *now* before technological imperatives pre-determine the selection for us.

Conclusions

- These public policy choices are not mutually exclusive.
- None of them obviate the critical need for strong and effective research ethics governance regimes.
- All of them require meaningful public engagement and stakeholder input to maintain public trust which remains the critical keystone to healthy, constructive relationships in our health system.

Conclusions

- The purpose of this paper is not to advocate for one policy option over another. Rather, it is intended to support informed discussions about the various policy choices available, the implications involved with each and the critical issues in need of further exploration and constructive debate.
- The opportunity is available *now* to avoid policy procrastination and effectively address some of these issues.

Building a Perinatal Surveillance System in Ontario

Jim Bottomley, Director, Ontario Perinatal Surveillance System

Abstract:

This presentation will discuss the evolution and growth of Ontario's maternal-newborn information system. The current and anticipated benefits of the system will be discussed, and challenges identified. The application process for prescribed registry status will be reviewed. Planned secondary uses for the data set will be reviewed, including processes required to ensure high quality, adequately de-identified, and timely datasets.

Bio:

Jim Bottomley obtained a BSCH from Queen's University in 1993 and a Master's of Health Administration from the University of Ottawa in 1999. He spent 3 years working as an Analyst at the Ottawa Hospital, and as a Regional Emergency Services Coordinator. Since then, Jim has led the management and development of Niday Perinatal Database, with the Perinatal Partnership Program of Eastern and Southeastern Ontario, located at the Children's Hospital of Eastern Ontario. Jim is currently the Director of the Ontario Perinatal Surveillance System (OPSS). OPSS is a network of clinical, data and planning leaders partnered to collect, analyze and report the outcomes of women and newborns receiving maternal-newborn care in Ontario. Current database partners of OPSS include the Niday Perinatal Database, the Ontario Midwifery Program Database, the Fetal Alert Network, the Newborn Screening Program and the Multiple Marker Screening Database. In 2008-09, the ministry will establish this partnership as a funded agency with registry status, able under Ontario's privacy legislation to administer programs, collect, research, analyse and report on perinatal data.

Ontario Perinatal Surveillance System

An Authoritative Perinatal Information System

Jim Bottomley, CHEO

Agenda

- Overview of OPSS
- Current and Future uses
- Privacy issues and other challenges
- Secondary Use Protocol and results

Surveillance in Canada

- **Long history of perinatal surveillance at local, regional, provincial and national level**

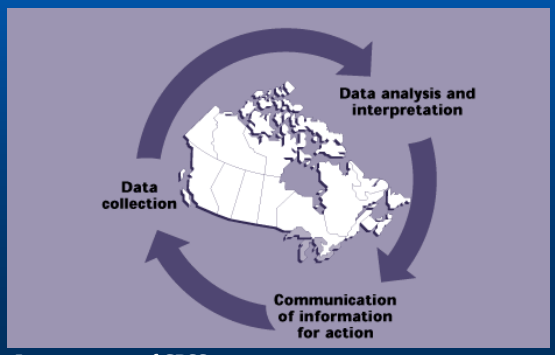


Image courtesy of CPSS

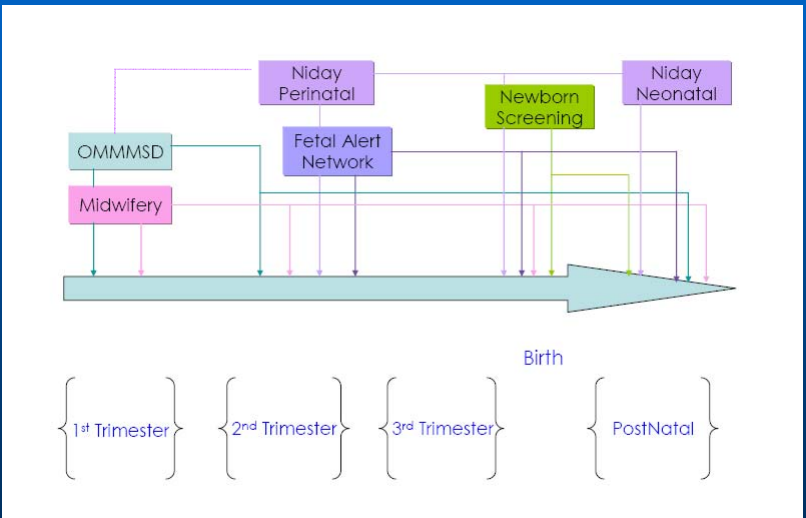
3

OPSS Overview

- **Collaboration of programs collecting maternal/ newborn data, including:**
  - **Niday Perinatal Database**
  - **Fetal Alert Network**
  - **Midwifery Program**
  - **Newborn Screening**
  - **Maternal Serum Screening**
- **To develop an integrated web portal that provides a common repository for all perinatal information**
- **Objective is to contribute towards achieving optimal health of mother, baby & families**

4

Data Continuum

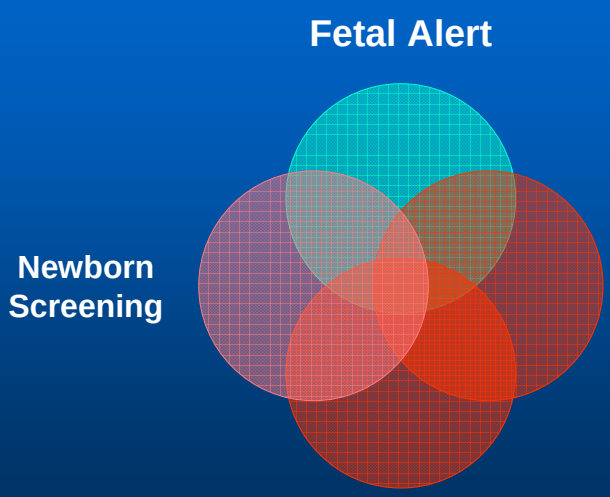


OPSS Rationale

- There are many rich sources of data used by each program for clinical care and surveillance, however:
  - There is duplicate data collection
  - Data element definitions are misaligned
  - There are few appropriate and timely health system planning and accountability measures
  - There is little data linkage and therefore unfulfilled value and lost potential
- Integration is needed to ensure a comprehensive data solution that will effectively support the activities and goals of the emerging maternal-newborn-child strategy of the MOHLTC

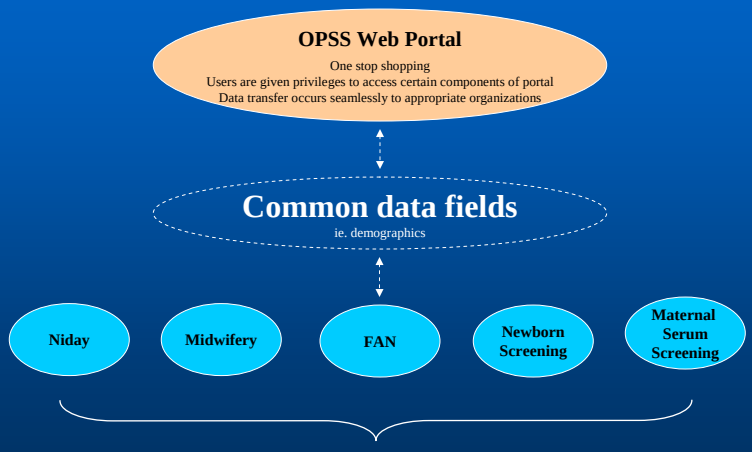
6

OPSS Databases



7

OPSS Data Vision



Privilege-based data retrieval

8

OPSS Objectives

- Support evidence-based strategy development and implementation
- Provide high quality data that supports innovative health planning and health system management / evaluation
- Eliminate redundancies and enhance efficiency
- Mandate data standards
- Improve linkages between data holdings
- Track individuals through the “continuum of care”
- Support research and innovation

9

OPSS Data Uses

- Many of planned applications would be considered “secondary uses” of data
- The challenge is to reach a practical balance between the improvement of health, the effectiveness of the health care services, and the right to privacy and confidentiality of personal information.
- Towards this effort, OPSS has:
  - Developed a new data architecture model for an integrated perinatal information system
  - Established a new governance model
  - With purpose of: applying for Registry status designation (or equivalent) to support OPSS objectives, able to collect, use and disclose personal health information in accordance with privacy legislation and data system standards

10

Secondary Uses

- Linked data will allow current programs to continue to manage and deliver their services, while also allowing the Ministry, LHINs and Public Health Units to:
  - develop responsive policies
  - improve evaluation and accountability in the system
  - support quality patient-centered care through service delivery improvements
  - promote health and healthy behaviours
  - support maternal and newborn disease prevention
  - inform human resources planning, and
  - create powerful hypothesis-generating research and innovation initiatives

11

Field of Dreams

"Build it, and they will come"

- Many unanticipated partners and potential usages
- Important to ensure robust yet flexible system, able to respond to new demands in the future

12

Challenges

- Before completing integration, important to evaluate risk of proposed OPSS system
- Various types of risk
  - Usability for end users (clinicians, hospitals, planners, etc)
  - Data quality
  - Technology
  - Privacy assurance

13

Privacy

- Given the sensitivity of the information in the OPSS, there are concerns about patient privacy and the need to obtain consent for secondary uses of that data.
- One method to address concerns is to de-identify data
- Protocol developed using data from the Niday Perinatal Database

14

De-id Protocol

- Evaluating Patient Re-identification Risk from an Ontario Perinatal Registry, by Khaled El Emam et al.
- If records cannot directly or indirectly identify patients, then not considered personal health information, and there would be no legislative requirement to obtain patient consent.

15

De-id Protocol

- The objective of this study is to evaluate the re-identification risk of data sets from the Niday registry, and what types of de-identification would be needed to ensure that this risk can be properly managed.
- Lessons learned from this study will transfer to all OPSS holdings, and will inform other similar initiatives

16

Niday Perinatal Database

- Developed in Eastern Ontario, by PPPESO, at CHEO
- Web-based database
- Captures 97% of births in Ontario
- “Real-time” perinatal data
- Partnership with hospitals, midwives, public health units, LHINS, MOHLTC, and other stakeholders
- Program management, benchmarking, CQI, planning, evaluation and research

17

Niday Database Indicator Framework

Risk factors and conditions influencing birth outcome
- •age
- •smoking
- •multiple pregnancy
- •presentation
- •age
- •health problems
- •previous CS
- •group B strep
- •reproductive assistance

Intrapartum interventions
- •monitoring
- •induction
- •epidural
- •forceps/vacuum
- •episiotomy, laceration
- •augmentation of labour
- •induction
- •cesarean
- •complications
- •steroid use
- •antibiotics
- •transfer
- •duration of second stage

Birth outcome
- •gestation
- •birthweight
- •APGAR 1, 5, 10
- •stillbirth
- •resuscitation
- •Hypoxia

Health service factors
- •first trimester visit
- •prenatal classes
- •care provider
- •birth in appropriate setting
- •length of stay in hospital

Infant health
- •Feeding
- •congenital anomaly
- •neonatal
- •death
- •hearing
- •health problems
- •jaundice
- •head circumference
- •surgery
- •SNAPS, TRIPS

18

Protocol Summary

- The Niday registry is considering disclosing parts of its database to external parties
- Because of concerns about privacy, the data custodian must ensure that the patient information in the disclosed database is de-identified.
- There are degrees of de-identification that can be applied. Too much de-identification may diminish the clinical utility of the data. Too little de-identification may be a breach of privacy.

19

Protocol Summary

- A risk analysis is performed to decide how much de-identification to apply. To conduct a meaningful risk analysis, the nature of plausible re-identification attempts needs to be understood.
- An individual or entity which attempts to re-identify a database is called an *intruder*:
  - Prosecutor re-identification risk
  - Journalist re-identification risk
- The focus in this analysis is with identity disclosure: ensuring that an intruder would not be able to determine the identity associated with any record in the disclosed database

20

Initial Analysis

- Assume a data request for Toronto births from Jan-Mar 07
- The intruder is a neighbor with basic information about:
  - Baby date of birth
  - Mother's age
  - Maternal postal code

21

Results - I

- Most of the records are unique – the risk of re-identification from these variables is very high
- Some form of de-identification is necessary before the data set can be released

22

Results - II

- At a maximum probability of re-identification of 0.2:
  - Postal code has to be generalized to region
  - Mother's age has to be generalized to a two year interval
  - Baby's birth date has to be generalized to quarter and year

23

Results - III

- Approximately 8% of the records have some suppression in them on these three variables
- Increasing the risk threshold from 0.2 to 0.4 does not have an impact on the extent of generalization

24

Thank-you

25

Disclosing Prescription Records to Commercial Data Brokers: A case study evaluating privacy risks

Regis Vaillancourt, Director of Pharmacy, Children's Hospital of Eastern Ontario

And Tyson Roffey, Chief Information Officer, Children's Hospital of Eastern Ontario

Abstract:

Pharmacies often provide prescription records to commercial data mining companies. This is done under the assumption that the records are de-identified. But there have been concerns about the ability to re-identify patients. Recently a large data mining company has requested prescription records from the Children's Hospital of Eastern Ontario (CHEO) as part of a larger national effort to develop a hospital prescription record database across Canada.

Dr. Vaillancourt and Mr. Roffey will present a case study which evaluates the ability to re-identify patients from a de-identified data set. A re-identification risk assessment on the requested data found that the probability of re-identifying patients in the original data set requested was very high. Vaillancourt and Roffey will describe how CHEO worked with privacy experts and the data mining company to find an optimal balance between re-identification risk and utility of the resulting data set.

Bios:

Regis Vaillancourt

Dr. Régis Vaillancourt is currently the Director of Pharmacy at the Children's Hospital of Eastern Ontario. Dr. Vaillancourt received his Bachelor of Pharmacy from the University of Laval in 1983, his hospital pharmacy residency certificate from the National Defense Medical Center (in affiliation with University of Toronto) in 1987, and his Doctor of Pharmacy from the University of Toronto in1995.

He joined the military in 1980, and during this time, has served as a military pharmacist in Valcartier, Québec; Ottawa, Ontario; and Chilliwack, B.C. He has worked as a staff pharmacist, as a clinical co-coordinator, and as a residency co-coordinator. He has also been employed as a pharmacist in a Field Ambulance, and as Commanding Officer of a medical equipment depot. Since completing his Doctor of Pharmacy degree, he has worked as the Canadian Forces Clinical Pharmacy Advisor, and Pharmacy Branch Advisor. He was responsible for directing all aspects of military pharmacy practice within the Canadian forces from 2002 to 2005.

Dr. Vaillancourt's dedication to the pharmacy profession has been recognized locally, nationally and internationally through numerous awards and appointments. In 2004 the Canadian Pharmacists Association named him the Canadian Pharmacist of the Year. In addition to pharmacy related accolades, he was awarded the Order of Military Merit by former Governor General, Adrienne Clarkson.

Throughout his career, Dr Vaillancourt has worked with the Ontario College of Pharmacists, l'Ordre des pharmaciens du Quebec, and has served as a board member for the National Association of Pharmacy Regulatory Authorities. Dr. Vaillancourt is currently a Vice President of the International Pharmaceutical Federation. He was President of the Canadian Society of Hospital Pharmacists in 2004-2005 and President of the Military and Emergency Pharmacy section from 2004-2008.

In order to maintain well-rounded clinical pharmacy skills, Dr Vaillancourt provides patient care on a part-time basis at Claude Veilleux Pharmacy in Hull, and provides clinical pharmacy support to the Nephrology and Chronic Pain pediatric clinics at CHEO.

Tyson Roffey

Tyson Roffey is currently the Chief Information Officer at CHEO (Children's Hospital of Eastern Ontario). Prior to joining CHEO in October 2007, Tyson was the Senior Director Business Development, Bell Centre for Healthcare Innovation. Among his most recent accomplishments, Tyson has led the strategy, business development and solution architect teams in the creation of a new IS solution for a national service provider supporting health care clients. Tyson's leadership skills and strong track record in innovation, development of IS solutions, and business transformations will prove indispensable to CHEO.

Evaluating Patient Re-identification Risk from Hospital Prescription Records

Dr Régis Vaillancourt, CHEO
DrKhaled El Emam, CHEO RI
Fida Dankar, CHEO RI
Tyson Roffey, CHEO

Outline

- Canadian medication utilisation databases
- Request
- Concerns
- Solution approach
- Conclusion

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Canadian Medication Utilisation Databases

IMS Health

- Multinational
- Market
  - Retail pharmacy
  - Warehouse
- Clients
  - Pharmaceutical
  - Government
  - Researchers
  - Focus on supply

Brogan Inc.

- Canadian
- Market
  - Retail pharmacy
  - Hospital Pharmacy
    - CAHO
- Clients
  - Pharmaceutical
  - Government
  - Researchers
  - Focus on prescribing

CHEO Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Brogan Inc.

Brogan Inc. provides timely market intelligence, insightful and in-depth research, and strategic solutions to current issues in the Canadian health care market.

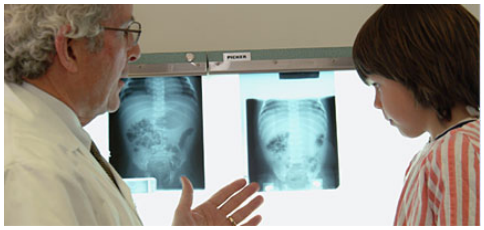
Serving all major pharmaceutical companies, insurers, and government organizations in Canada, Brogan Inc. offers solutions to help our clients leverage the power of business intelligence to:

· Detect and exploit emerging trends
· Make proactive decisions
· Fine tune strategies for success, and
· Gain competitive advantage

CHEO Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Outline

- Canadian medication utilisation database
- Request
- Concerns
- Solution Approach
- Conclusion



Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Request

- CAHO Agreement
  - Council of Academic Hospitals of Ontario
  - Agreement with Brogan

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Request

- Fields Requested (summary)
  - Patient age
  - Patient gender
  - Forward Sortation Area- Postal Code
  - Admission date
  - Discharge data
  - Diagnosis
  - Specifics about the dispensed drug

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

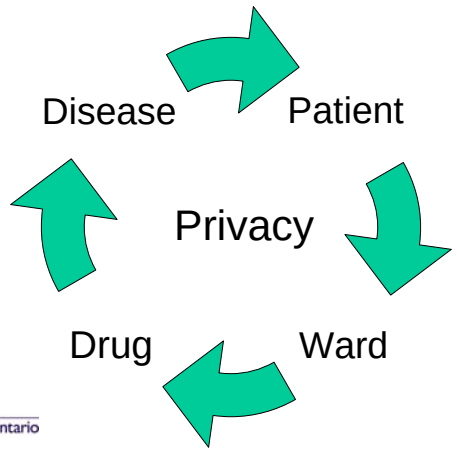
Outline

- Canadian medication utilisation database
- Request
- **Concerns**
- Solution Approach
- Conclusion

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Concerns

- Linking databases
  - Pharmacy- CIHI



Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Concerns

Examples

• Valtrex ™	Herpes
• Insulin	Diabetes
• Lipitor ™	Hyperlipidemia
• Prozac ™	Depression
• Valium ™	Anxiety
• Viagra ™	Pulmonary hypertension

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Concerns

Original Database to Disclose

	IDENTIFYING VARIABLE	QUASI-IDENTIFIERS		
ID	Name	Gender	Year of Birth	Test Result
1	John Smith	Male	1959	+ve
2	Alan Smith	Male	1962	-ve
3	Alice Brown	Female	1955	-ve
4	Hercules Green	Male	1959	-ve
5	Alicia Freds	Female	1942	-ve
6	Gill Stringer	Female	1975	-ve
7	Marie Kirkpatrick	Female	1966	+ve
8	Leslie Hall	Female	1987	-ve
9	Bill Nash	Male	1975	-ve
10	Albert Blackwell	Male	1978	-ve
11	Beverly McCulsky	Female	1984	-ve
12	Douglas Henry	Male	1959	+ve
13	Freda Shields	Female	1975	-ve
14	Fred Thompson	Male	1967	-ve

De-identification

	QUASI-IDENTIFIERS		
ID	Gender	Decade of Birth	Test Result
1	Male	1950-1959	+ve
2	Male	1960-1969	-ve
4	Male	1950-1959	-ve
6	Female	1970-1979	-ve
7	**Female**	**1960-1969**	**+ve**
9	Male	1970-1979	-ve
10	Male	1970-1979	-ve
11	**Female**	**1960-1969**	**-ve**
12	Male	1950-1959	+ve
13	Female	1970-1979	-ve
14	Male	1960-1969	-ve

Disclosed Database

Matching

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Concerns

- The First 5 Minutes
  - Data for the 18 months was obtained
  - We were able to name a patient from those same fields within 5 minutes of getting the data set
  - Need to do a detailed analysis of re-identification risk

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Concerns

Privacy officer's first reaction is no

CHEO's Enablement philosophy

Clinical need for the information

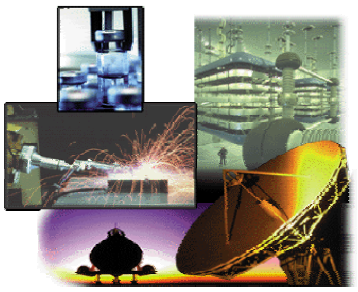
Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Outline

- Canadian medication utilisation database
- Request
- Concerns
- **Solution Approach**
- Conclusion

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

- Risk Assessment Software



http://www.probabilistic-risk-assessment.com/images/collage.gif
http://software-testing-zone.blogspot.com/2008/06/what-to-test-pareto-analysis-high-risk.html

Focus on:

– Demographics
– External Intruder Scenario

Our Approach

- Risk Threshold Assessment

  0.2

  – There is a 1 in 5 chance that an individual can be re-identified

  0.4

  – There is a 1 in 2.5 chance that an individual can be re-identified

CHEO Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

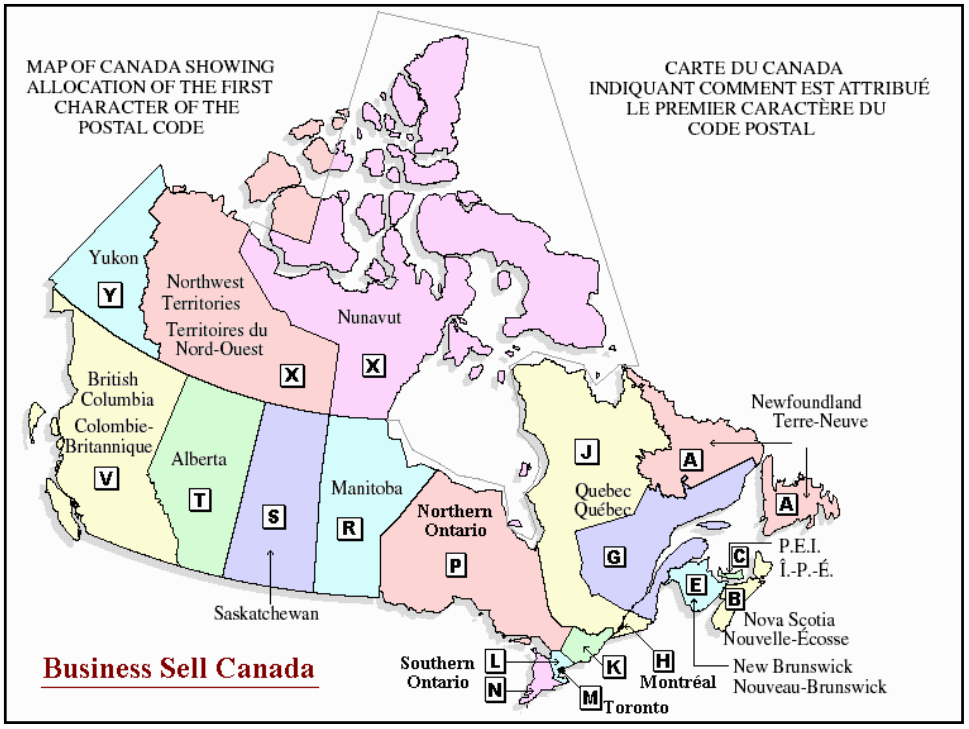
Fields Requested (summary)

- Patient age
- Patient gender
- Forward Sortation Area- Postal Code
- Admission date
- Discharge data
- Diagnosis
- Specifics about the dispensed drug

CHEO Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Variable Granularity to be Included in Disclosed Database						Percent of Records with Cell Suppression	
Admit Date	Discharge Date	Length of Stay	Postal Code	Age	Gender	Baseline Risk Scenario *(at a risk threshold of 0.2)*	Lower Risk Scenario *(at a risk threshold of 0.4)*
day/ month/ year	day/month/ year	--	FSA	days	M/F	100%	100%
day/ month/ year	day/ month/ year	--	region	days	M/F	100%	100%

CHEO Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario



Clinical Value of Data

Quasi-identifier	Maximum Acceptable Generalization
Gender	No generalization possible
Age	Days to weeks
Postal Code	First character of the postal code
Admission/discharge dates	Changed to length of stay and admission quarter

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Variable Granularity to be Included in Disclosed Database						Percent of Records with Cell Suppression	
Admit Date	**Discharge Date**	**Length of Stay**	**Postal Code**	**Age**	**sex**	**Baseline Risk Scenario** *(at a risk threshold of 0.2)*	**Lower Risk Scenario** *(at a risk threshold of 0.4)*
month/ year	month/ year	--	region	days	M/F	40.5%	29.2%
quarter/ year	quarter/ year	--	FSA	days	M/F	81.4%	64.7%
quarter/ year	quarter/ year	--	region	days	M/F	22.1%	15.3%
quarter/ year	quarter/ year	--	region	days	M/F	--	13.8%
quarter/ year	--	days	region	weeks	M/F	--	14.9%

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Our Solution

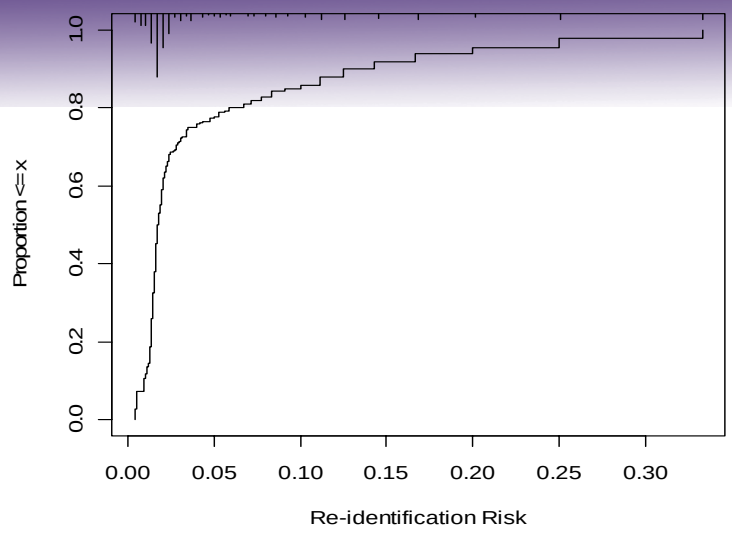
- Key Variables Disclosed
  - Gender
  - Length of stay in days
  - Quarter and year of admission
  - Patient's region (first character of the postal code)
  - Patient's age in weeks

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

N = 10,364

Quasi-identifier	Number of records with the quasi-identifier suppressed	Percentage of total records with the quasi-identifier suppressed
Gender	117	1%
Age	1177	11.3%
Region	475	4.6%
Admission Date	548	5.3%
Length of Stay	398	3.8%

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario



Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Outline

- Canadian medication utilisation database
- Request
- Concerns
- Solution Approach
- **Conclusion**

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Leverage Acceptable Standards

- Risk Threshold Assessment
  - 0.2
    - There is a 1 in 5 chance that an individual can be re-identified
  - 0.4
    - There is a 1 in 2.5 chance that an individual can be re-identified

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Why use PHI ?

- Use Anonymized Data:
  - No legislative requirement to obtain consent for using and sharing the data
  - Many REBs will waive the consent requirement if a dataset is de-identified
  - Reduced liability should a breach occur
  - Reduce the number of issues that come up and have to be addressed during Privacy Impact Assessments

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Mitigating Controls

- What additional controls were required to make this work:
  - Regular third party privacy/security audits
  - Breach notification protocols must be in place
  - Restrictions on further distribution of raw data
  - Data destruction provisions

CHEO Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Focus on Enablement

- People
  - Ensure people have tools and knowledge
- Process
  - Leverage existing processes to ensure adoption
    - Eg. Research Ethics Board and Standard Privacy processes
  - Privacy as a culture is part of the solution not the problem
- Technology
  - Ensure technology tools add value

CHEO Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Rest Easy

Questions ?

Children's Hospital of Eastern Ontario
Centre hospitalier pour enfants de l'est de l'Ontario

Session 2C: Personal Health Records

Session Chair: Bradley Malin, Assistant Professor, Vanderbilt University

Chair 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.

Electronic Health Records: A patient's perspective regarding content, support, access & security

Kevin J. Leonard, MBA, Ph.D., CMA, Associate Professor, University of Toronto

Abstract

The healthcare system is beginning to provide patients access to their own health information, primarily within Electronic Health Records (EHRs) and Patient Health Records (PHRs). As these systems start to be implemented, many questions arise regarding content, support, access and security. As a result, patients must be involved in the process of designing, developing, implementing and evaluating EHRs so as to ensure their success. One major concern relates to personal health data and information. In this talk, we will present research findings pertaining to the patient perspective and conclude with recommendations for on-going research and development. One recurring observation is that as more and more patient health information becomes available, additional education programs will have to be developed to safely activate and empower patients as partners in their care.

Bio

Kevin received his Ph.D. from the Joint Doctoral Program in Montreal where he specialized in Statistics and Information Systems Theory for Business. In 1996, Kevin joined the Department of Health Policy Management and Evaluation at the University of Toronto. He has two primary areas of research: (i) the implementation of electronic health records (EHRs) along with researching issues pertaining to the development and implementation of patient focused information technology (Patient Health Records -PHRs); (ii) the creation and implementation of metrics for performance measurement of the Information Technology investment within healthcare (Improve-IT).

Electronic Health Records: The Patient Perspective re Content, Support, Access & Security

November 3, 2008

Kevin J. Leonard MBA, Ph.D., CMA

Associate Professor, Dept of Health Policy, Management and Evaluation, University of Toronto

Research Scientist, Centre for Global eHealth/UHN

Founding Director, Patient Destiny

Director, IMPROVE-IT Institute

eHealth includes:

- All uses of IS/ICTs in healthcare
- EHR's and PHR's
- CPOE
- CDR – data repositories
- DSS – decision support
- Patient management systems
- PACS – digital diagnostic imaging

eHealth can provide value by:

- Providing information to support decision making
- Providing metrics to assist managing "what you measure" (i.e., evaluation)
- Providing insight into the benefits that emanate from IT Spending
- Identifying poor data quality
- Improving health outcomes???

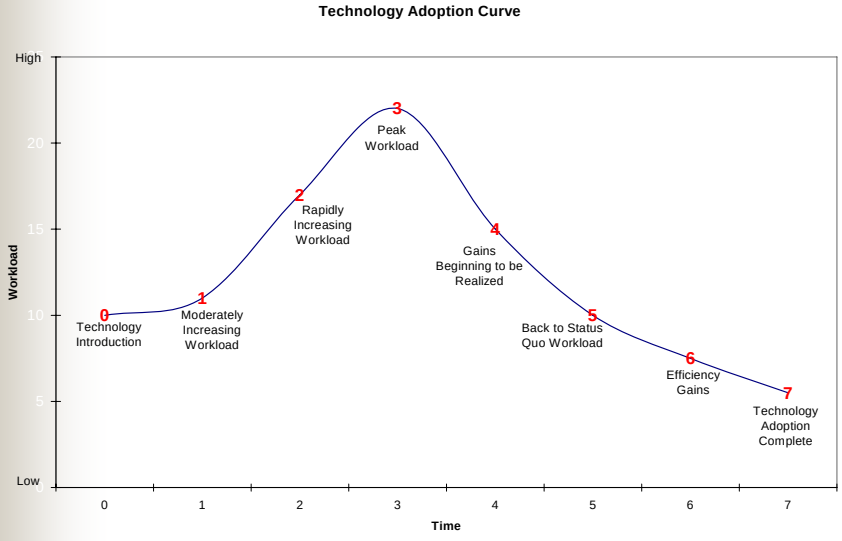
Evolving societal trends affecting healthcare

- change and changing technology
- rising consumerism and demand for information
- awareness of performance measurement and evaluation

Critical Success Factors - CSFs

1. amount of resistance to change (i.e., presence of industry experience using technology),
2. amount of training before/during the transition,
3. amount of buy-in from the different stakeholder groups (e.g., consumerism),
4. level of end-user influence during design, development and early stages of adoption,
5. presence of effective reporting on the status of the outcome measures/performance,
6. effectiveness in dealing with the "breaks"

Leonard, K.J. (2004), "Critical Success Factors Relating to Healthcare's Adoption of New Technology: *A Guide to Increasing the Likelihood of Successful Implementation*", Healthcare Quarterly, Volume 7, Number 2, p. 72-81.



Survival of our healthcare system requires patient involvement

- Decision makers need info to make good decisions
- Patients must be able to access their info in there are to help manage their care
- Paper documents within a fragmented health delivery systems makes consistent access infeasible

Patient Destiny !

Patients are destined to be responsible for their own healthcare

Health system has been slow to accept patient access – to see the benefits

Patients must be incented and educated about what is possible

Patients are no longer isolated

What is the patient's role?

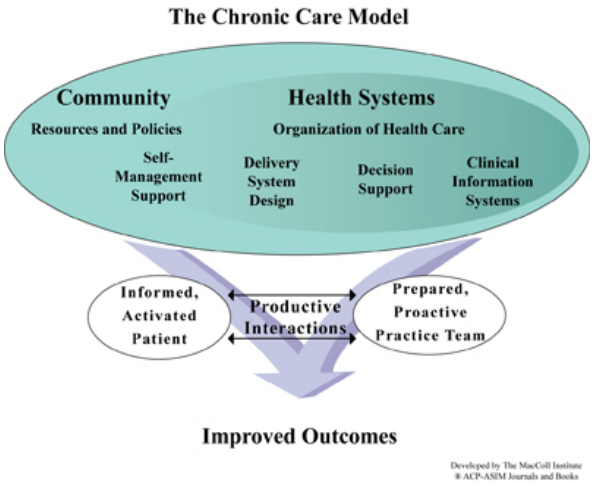
"We doctors do nothing. We only help and encourage the doctor within."

-- Albert Schweitzer

The Patients' Role

- Patients today are capable of alleviating some of the "volume delivery stress" on the system by helping to manage their care.
- This is referred to as The Chronic Care Model (estimated that $1 spend saves $2-$4 in healthcare delivery costs)
- Coined the term 3C (consumers with chronic conditions)

Wagner EH. Chronic disease management: what will it take to improve care for chronic illness? Eff Clin Pract. 1998;1:2-4



The Patients' Role - continued

- 70-80% of healthcare system costs relate to chronically ill (approx 30-40% of population).
- Also, they can put pressure on the system to evolve and change … and best way to advance Information Technology adoption is by the public (both the healthy and the ill) putting on the pressure to improve communication & use of IT

Cost of 3C

- 70-80% of healthcare system costs relate to chronically ill (approx 30-40% of population).
- 133 million in the US are 3C (Robert Wood Johnson Foundation - which is approx 40-45% (improvingchroniccare.org)
- Estimated 12.8-14.4 million Canadians with 3C (approx 13.5 million patients)
- About $100 billion spent on 3C in Canada (out of $150+ billion healthcare spend)

Canadian Cost Savings Arithmetic

- approx $150 billion total healthcare spend
- 50% of time/spend getting care
- 50% of time/spend getting information
- approx 2/3 of spend attributable to 3C
- so $50 [$150 x 0.5 x 0.66] billion spend on providing information to 3C (i.e., test results, care advice, repeat prescriptions)
- a mere 10% improvement in info transfer for the 3C would result in savings of $5 billion
- Does not include resulting savings in care, treatment – i.e., healthcare delivery costs

The 3C Patients

- 3C patients must be educated and "incented" to help alleviate some of the "volume delivery stress" on the system by partnering with care providers.
- Patients are destined to manage their care and become empowered
- No longer just the patient – but the "Patient Team" consisting of caregivers

The 3C Patients

- 3C patients must be educated and "incented" to help alleviate some of the "volume delivery stress" on the system by partnering with care providers.
- Patients are destined to manage their care and become empowered
- No longer just the patient – but the "Patient Team" consisting of caregivers

Research on Patient Perspective

- Patients are not as concerned with:
  - Confidentiality
  - Sacrificing care for privacy
  - Moving to e-records
  - Sharing records
- Patients are concerned with:
  - Wait lines, waiting times
  - Getting a doctor
  - Getting the best treatment
  - Quality – patient safety

What do we mean by health outcomes?

- financial indicators
- productivity
- patient outcomes
  - complying with best practice guidelines
  - performance on health indicators (HA1C)
  - patient satisfaction
  - hospital outcomes (re-admits or LOS)
  - patient safety

Patient Destiny leads to Patient Safety:

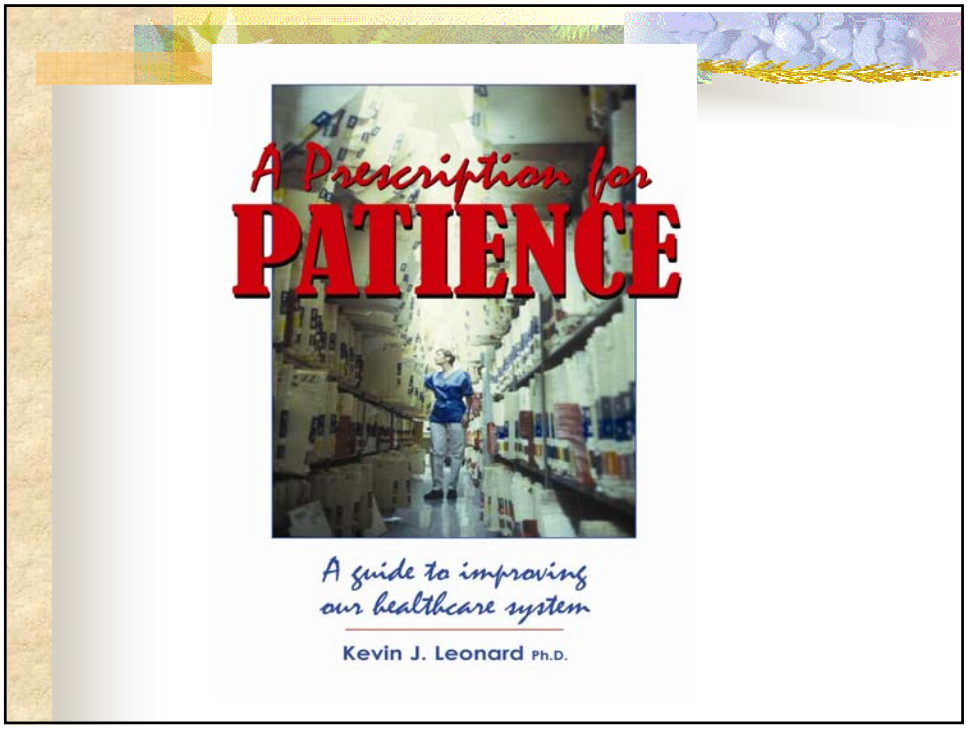
- Patients can do audit function
- Help improve compliance with drug and treatment regimens
- Increase dialogue between patient and providers resulting in better educated and more informed patients
- Increase sharing of info and experience among patient team – reducing strain on system/clinicians

We need the research – now!!

- Patients must be involved in design of PHRs
- How do we support patients accessing their electronic health information?
- Who controls access to their record?
- Does this lead to improved patient outcomes?
- Does this lead to improvement in patient safety outcomes?
- How does more “record ownership” address the privacy issues?
- Patients MUST be able to take action and change behaviour in a CDM model

Patients need representation!

- Patients must be represented by a formal organization
- This organization must represent both the ill (chronic and otherwise) and the healthy
- This organization must be recognized as such and invited to the table with other organized stakeholders – CMA, CNA, OHA
- The INFORmed Society



Electronic Health Records: The Patient Perspective re Content, Support, Access & Security

November 3, 2008

Kevin J. Leonard MBA, Ph.D., CMA

Associate Professor, Dept of Health Policy, Management and Evaluation, University of Toronto

Research Scientist, Centre for Global eHealth/UHN

Founding Director, Patient Destiny

Director, IMPROVE-IT Institute

Addressing Privacy Challenges in Putting Personal Health Information Online

George Scriban, Senior Global Strategist, Consumer Health Platform, Microsoft Corporation

Abstract:

In October 2007, Microsoft launched HealthVault, an online service that allows people to collect, store, and share their personal health information, and health information for their families. The promise of digital, connected health information is enormous—health information is truly valuable when it is shared with caregivers and clinicians—but HealthVault had to take into account the privacy concerns consumers have with putting some of their most personal information online. We'll examine the process Microsoft used to help them design privacy into HealthVault, and discuss the challenge of creating a trustworthy consumer health platform and ecosystem.

Bio:

George Scriban has been involved in the business side of technology for 15 years. Today, as senior global strategist for Microsoft® HealthVault, the company's consumer health platform, Scriban is responsible for product strategy, marketing and planning for the core platform in such areas as privacy policies, security strategy, and compatibility with industry standards.

Before joining Microsoft in August 2007, Scriban served as research director with Gartner Inc.'s The Research Board Inc., a New York-based private think tank serving senior technology executives from Fortune Global 200 organizations. There Scriban ran the Digital Security Board, which delved into issues of strategic importance to member companies that included CIGNA, Merck & Co. Inc., Bank of America, The Boeing Co., BP plc, GlaxoSmithKline plc, Altria Group Inc. and Shell.

Before his work with Gartner, Scriban was product manager for search and Web analytics products at 24/7 Real Media and sales director for Insight First, which 24/7 Real Media later acquired. He has also served as director of Business Development and Strategic Relationships at OpenCola and vice president of Marketing and Sales at e-mail response management startup ESPONSIVE. He began his career in sales and marketing management at Andyne Computing Ltd., working in a variety of roles as the company grew from fewer than 20 employees to more than 250.

Scriban holds an undergraduate degree in politics and English literature from Queen's University in Canada.

Microsoft HealthVault

Addressing privacy challenges in
putting personal health information online

HealthVault

Yesterday

BIOMETRIC DATA

DATA MANAGEMENT/
DATA ANALYSIS

MEDICAL ANALYSIS

HealthVault

Today

BIOMETRIC DATA

DATA MANAGEMENT/ DATA ANALYSIS

MEDICAL ANALYSIS

Microsoft HealthVault

3

Tomorrow

BIOMETRIC DATA

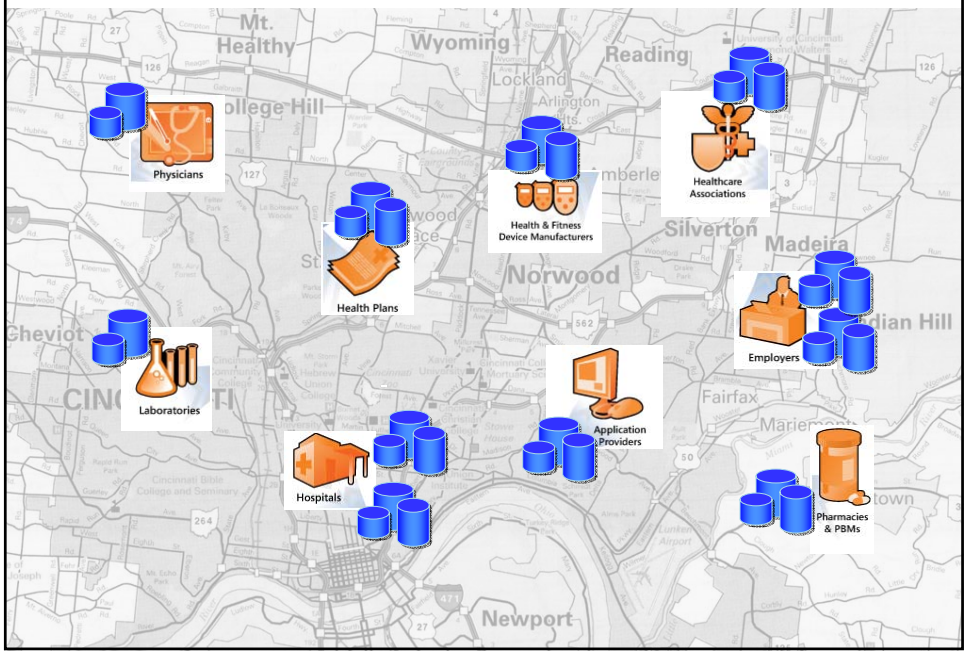
DATA MANAGEMENT/ DATA ANALYSIS

MEDICAL ANALYSIS

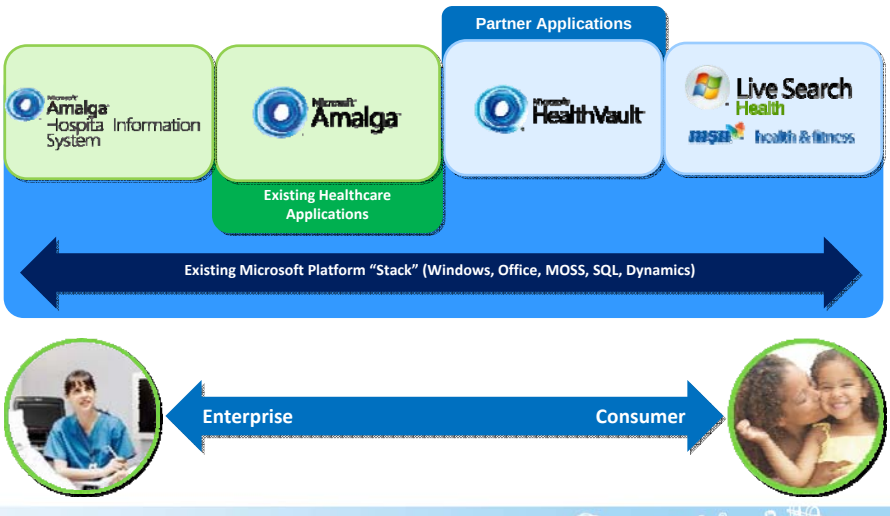
Microsoft HealthVault

4

Silos In The Ecosystem



Microsoft Health Solutions



Microsoft HealthVault

Beyond The Standards Debate

Why is healthcare still waiting to achieve interoperability?

- Today's efforts are focused on creating + evolving standards
- We need to move beyond this effort

De jure Standards

Translation Based Interoperability

Unlocking the Data

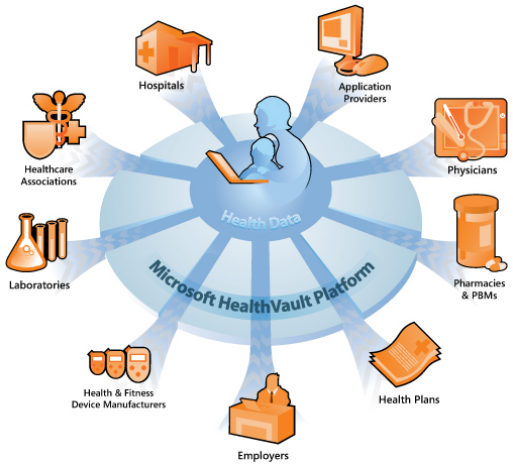
Put People in the Equation

Microsoft HealthVault

7

What is HealthVault?

A platform for consumer empowerment and engagement with and through their personal health data



Microsoft HealthVault

What is HealthVault?

- A cloud service from Microsoft that helps people collect, store, and share their personal health information.
- A web-based platform for new, valuable online health, wellness, fitness, and diet services tailored to people's health information.
- Data can come from providers, pharmacies, plans, government, employers, labs, equipment and devices, and from consumers themselves.

Microsoft HealthVault

HealthVault: Software + Services Platform

SOFTWARE

Microsoft HealthVault Connection Center

HealthVault Connection Center is a utility that allows users to add data from health and fitness devices such as heart rate monitors, blood pressure monitors, peak flow meters, glucometers, and pedometers.

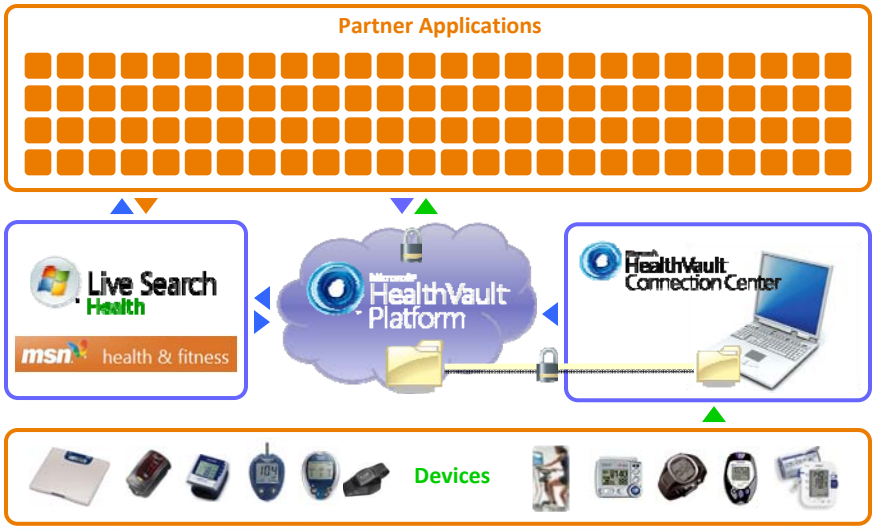
SERVICES

Microsoft HealthVault is an online personal health database with a set of XML interfaces that allows third parties to create valuable health, wellness, and fitness services for HealthVault users.

Microsoft HealthVault

11

HealthVault Platform Architecture



Microsoft HealthVault

12

Design Principles Of HealthVault

Privacy and Security Focused

Inclusive of Industry Standards

Free for Users and Developers

Microsoft HealthVault

14

Creating our privacy strategy

- Microsoft corporate privacy policies set a baseline.
- A survey of global health privacy regulations raised the bar further.
- Engagement with consumer privacy advocates, health and otherwise, was incorporated into HealthVault product architecture and privacy policies.
- We continue to engage with privacy influentials globally to refine our privacy efforts.

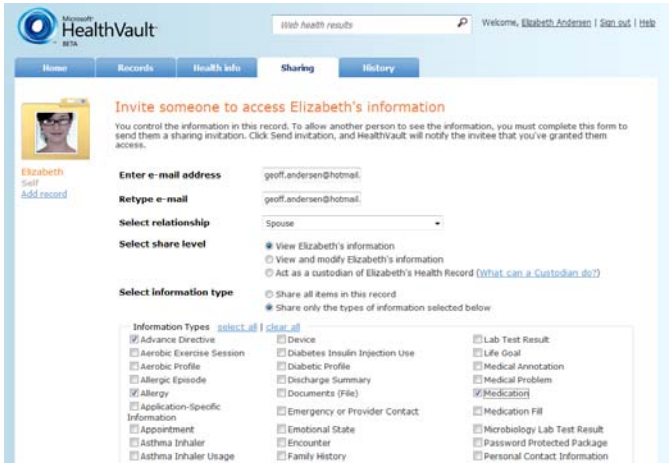
Microsoft HealthVault

Our privacy commitment

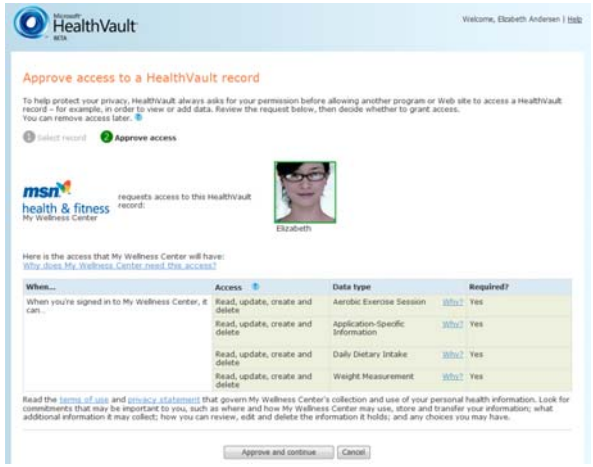
1. The Microsoft HealthVault record you create is controlled by you.
2. You decide what goes into your HealthVault record.
3. You decide who can see and use your information on a case-by-case basis.
4. We do not use your health information for commercial purposes unless we ask and you clearly tell us we may.

Microsoft HealthVault

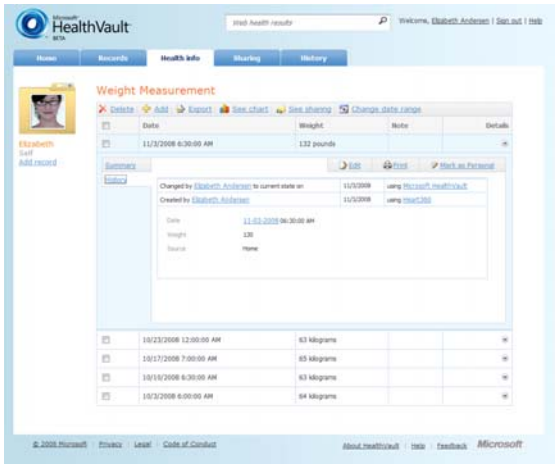
Sharing your information



Authorizing applications



Complete history



Microsoft HealthVault

Operational security

- Microsoft's data centers are high-security operations, certified to international standards such as ISO 27001.
- HealthVault's systems operate with extra precautions:
  - Physically separate, locked cabinets
  - Logically segmented network traffic
  - All communication between system components is encrypted
  - Only essential Microsoft personnel are permitted access to HealthVault systems
  - All system activity is logged

Microsoft HealthVault

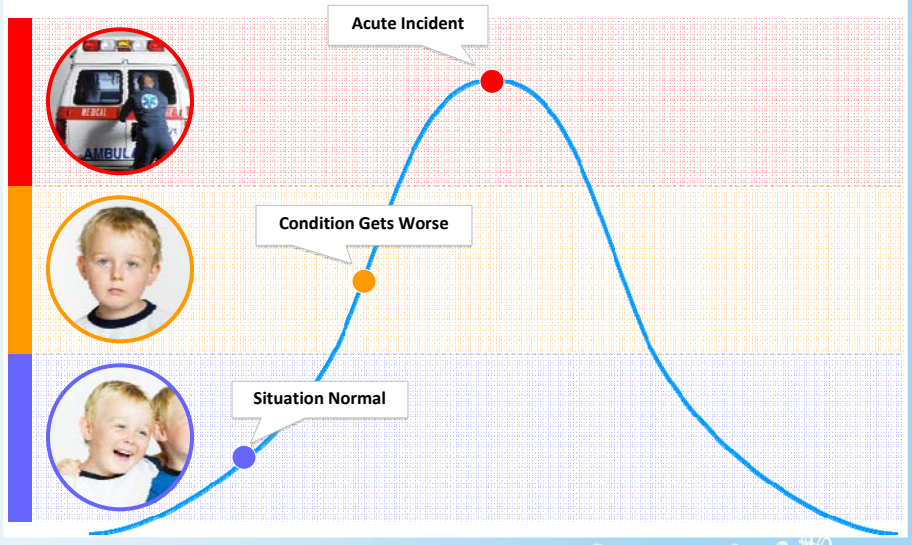
Trustworthy ecosystem

- All third-party solution providers must sign a solution provider agreement (SPA) which outlines their privacy obligations to consumers.
- Unless covered by HIPAA, they must maintain and comply with a privacy statement at least as protective of the security, confidentiality, integrity, and accuracy of End-User Data as the HealthVault Privacy Statement.
- All communication between solution provider applications and HealthVault are encrypted.

Microsoft HealthVault

21

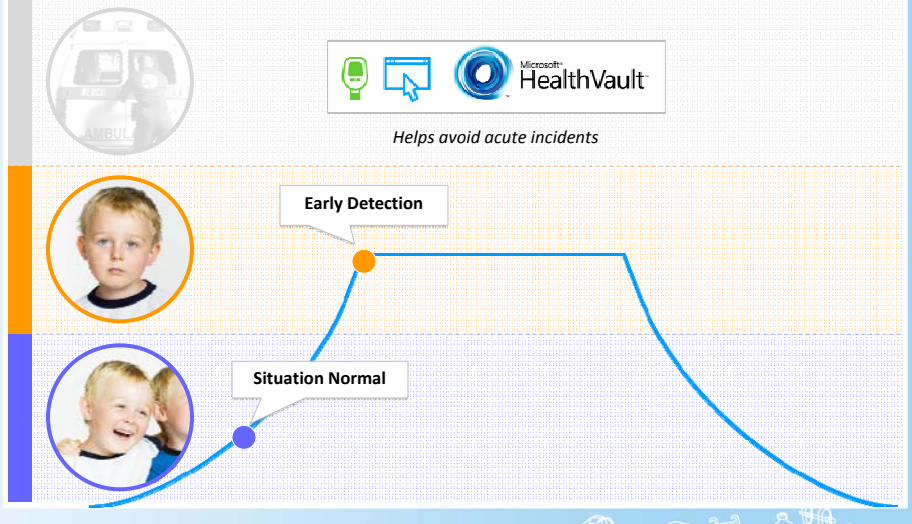
Chronic Care → Acute Care Cycle



Microsoft HealthVault

23

Secondary Prevention: Flattening the Curve

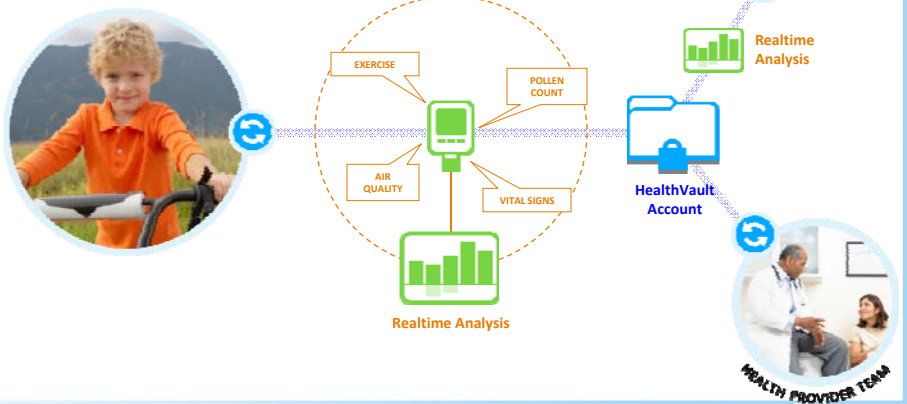


Microsoft HealthVault

24

Jesse: Asthma

Jesse is an active 9 year old with asthma who loves to play outside. His asthma is usually triggered by exercise. Because of the integration of technologies, he is able to participate in a outdoor activities that used to only be a dream for kids with his condition.



Microsoft HealthVault

25

Microsoft

Contact: gscriban@microsoft.com

Microsoft HealthVault


Microsoft
Your potential. Our passion.™

Is Privacy Dead?

Benjamin Heywood, Co-founder & President, PatientsLikeMe

Abstract:

Ben will discuss how sharing real-world, real-time healthcare experiences and outcomes can shake up (and wake up) healthcare today. In his presentation, he will examine how the inaccessible nature of today's healthcare data can slow down research. Launched in 2006, PatientsLikeMe now has more than 20,000 patients sharing structured data about their health. Join Ben to see what can happen when we become a little less privacy-focused, and a lot more open.

Bio:

Benjamin Heywood has served as the president and director of PatientsLikeMe since its inception in 2004. His professional experience spans a diverse set of operational areas including successful ventures in the medical device industry, the entertainment industry, and in speculative residential real estate development. After graduating from Massachusetts Institute of Technology (MIT), Heywood moved to Silicon Valley to work for Target Therapeutics, the leading designer and manufacturer of microcatheter-based products for the treatment of stroke.

After significant involvement in both manufacturing and product design, he eventually moved into Business Development until Boston Scientific acquired the company. Prior to co-founding PatientsLikeMe, Heywood was a Creative Executive at the film and television production company SideStreet Entertainment. While working in Hollywood, he produced an award winning short film, Flush, and worked in both production and script development on numerousfilms. A highly regarded thought leader in the Health 2.0 industry, Heywood is a frequent speaker at conferences and source for the news media on topics in this space. He has been quoted in *New York Times, New York Times Magazine*, Newsweek, CNNMoney and numerous trade publications. Heywood earned his Bachelor's degree in Mechanical Engineering from MIT and received his MBA from the UCLA Anderson Graduate School of Management.

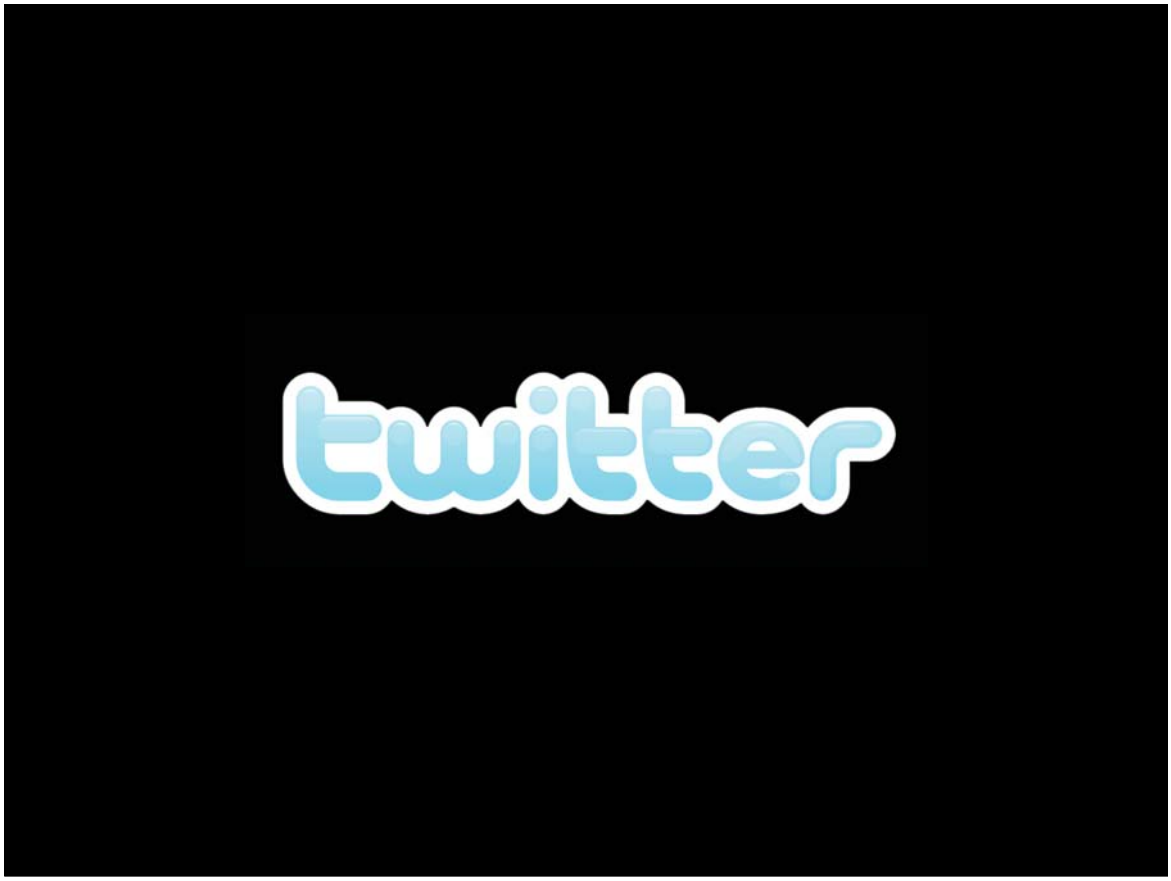
patientslikeme™

Benjamin Heywood

November 3rd, 2008

Is Privacy Dead?


facebook


twitter

What is PatientsLikeMe?

Online communities

Patient Reported Outcomes	Longitudinal Structured
Treatments	Quantitative
Symptoms	Qualitative

What is PatientsLikeMe?

For Profit

Insights

Access

Privacy Policy

Openness Philosophy

We believe sharing your healthcare experiences and outcomes is good. Why? Because when patients share real-

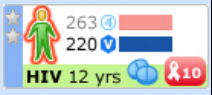

alsking101
Male, 38 years
Newton, MA
ALS: 9 yrs
Diagnosis Summary
Onset: Arms
First symptom: Nov 1997
Diagnosis: Jan 1998
Deceased date: Nov 26, 2006
Updates
Last updated: Oct 15, 2006
ALS Condition
Onset
Diagnosis
Deceased
Last Update
Jan 98
Jan 99
Jan 00
Jan 01
Jan 02
Jan 03
Jan 04
Jan 05
Jan 06
FRS: 0
(latest: 10/01/06)
Progression rate percentile
5-10th (rapid)
10-25th
25-75th (average)
75-90th
90-95th (slow)
FRS
Score: 30
Date: Oct 01, 2000
FVC: 5%
(latest: 02/06/06)
Warning Levels
warning
severe
FVC (%)
Treatments
Prescription
Reasons Taken
slow my ALS progress
general health
specific symptom
other
100 mg daily
80 mg
1200 mg daily
Rilutek (riluzole)
Elavil (amitriptyline)
CoQ10
Feeding Tube
Symptoms
Primary Symptoms
Severity of Symptoms
none
mild
Anxiety
Constipation
Depression

Our mission is to improve the lives of patients through new knowledge derived from shared real-world experiences and outcomes

The impact of a drug holiday in HIV

HIV Community

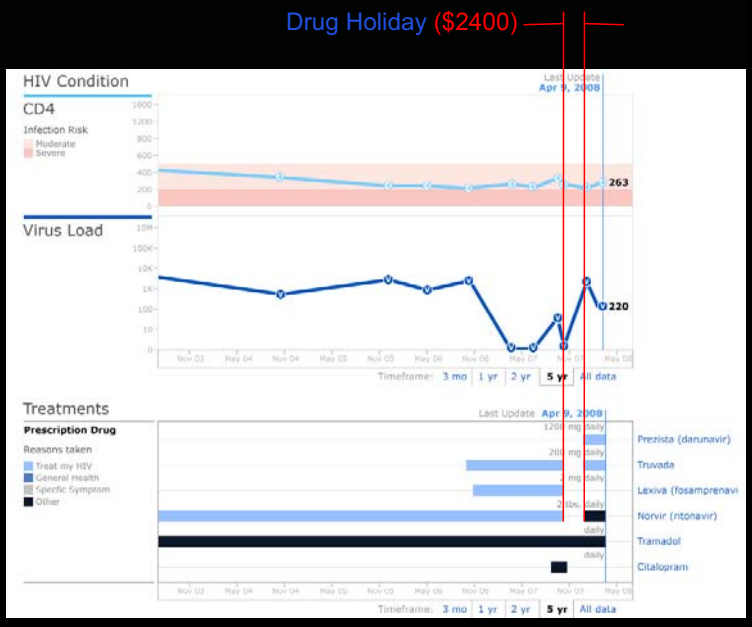
Anyone who wants to see what happens on a 2 month drug holiday just look at my updated VL and CD4 count.



After being taken off of old meds to track down some unwanted side affects. My VL spiked from undetectable up to 7,360 in a two month period.

Having been on new meds for 28 days my VL dropped precipitously. As of last Tuesday 220.

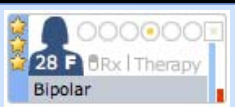
I must say also that a drug holiday is not what it once was. Not taking 8 relatively small easy to swallow pills a day just does not compare to not taking 30 giant rubberized stick to the back your throat pills a day. I just kinda feel like I am on a drug holiday all the time by comparison.



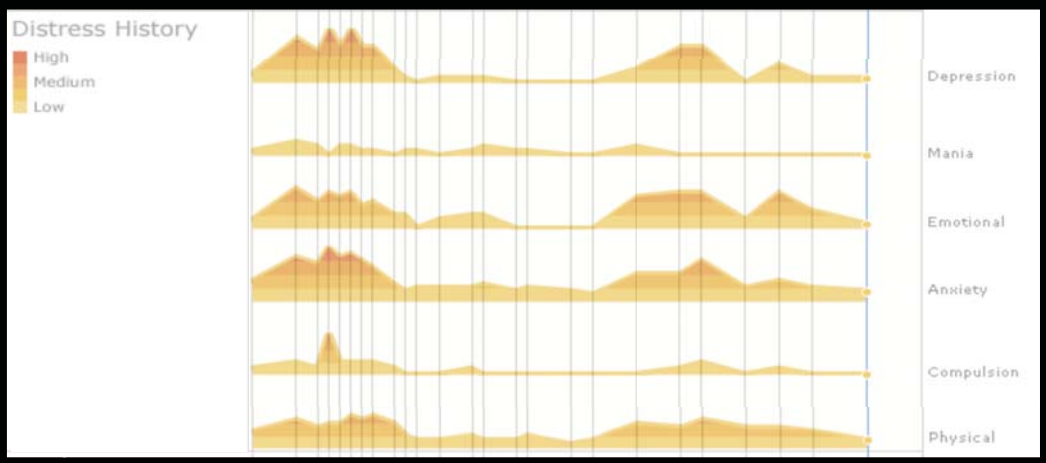
Using shared data to drive treatment decisions

Information Based Insights

Mood Community



PatientsLikeMe is the main reason that I concluded I had been mis-diagnosed depressive, instead of bipolar, and just recently decided to try new medication.



Peer disease management

ALS Community

The first thing that I thought might be your Problem is malnutrition. Man, you're losing weight crazy fast. I think you better consider getting Peg tube if you desire. They are easy to care for and are literally a life saver. What are your thoughts on this?

Core Values

Honor Patients' Trust

Openness

Transparency

Create Wow!

Is this safe?

Where does this lead?

= Privacy?

Forum Post:
Selling our MS history

20:1

SELLLLLLLL!!! SELL SELL SELL SELLLLLLLLL
and then SELL IT AGAIN!!!

-PatientsLikeMe Member

As for me, I am very comfortable with what PLM is doing.

-PatientsLikeMe Member

They are TOTALLY and completely up front about it with PLM members is ABSOLUTELY fine with me.

-PatientsLikeMe Member

It's a win/win as far as I am concerned.

-PatientsLikeMe Member

Sell, Sell, Sell. I've already been given much in return for my information. That we would get other bonuses for the selling of our aggregate data, I say yummy, all the better!!

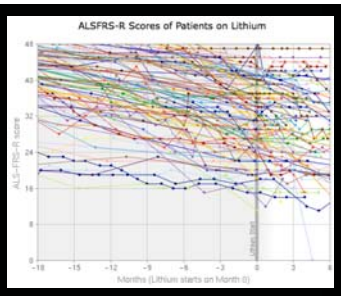
-PatientsLikeMe Member

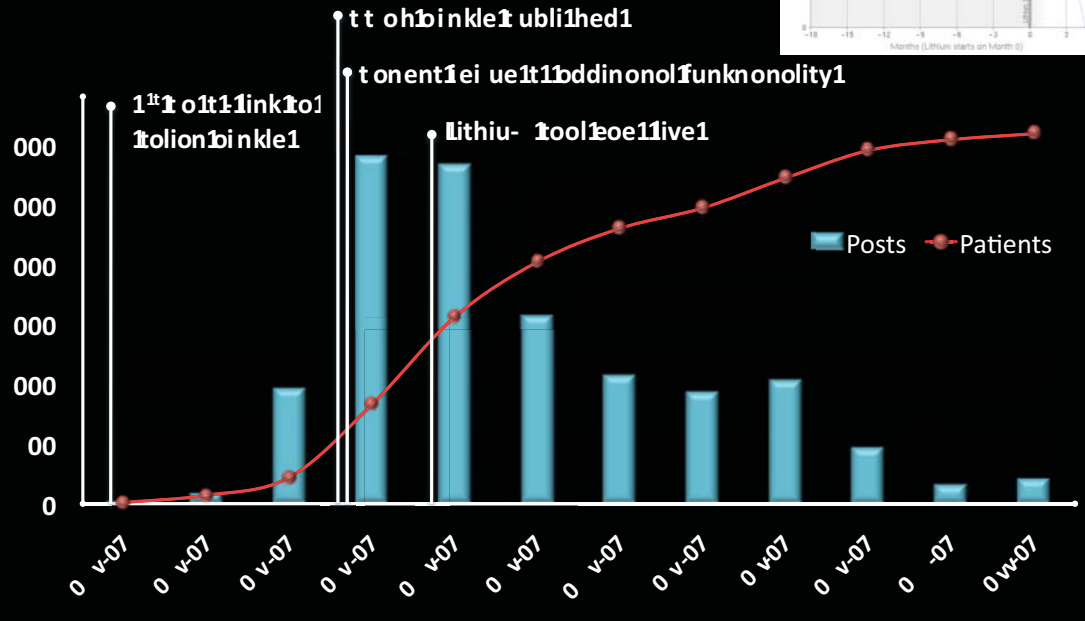
The Genetic Information Nondiscrimination Act (GINA) was signed into law by President Bush on May 21, 2008.

What is the medical information equivalent?

Risk vs Reward

Can patients answer clinical questions as a group?





bheywood@patientslikeme.com