VA Security Workshop 2010
Information Security, Putting the Pieces Together. . .

the intersection of privacy and security

September 16, 2010
Deborah C. Peel, MD
patientprivacyrights

security and privacy

clinical justification for security

- patients' expectations/rights
- liability/reputation

privacy-enabling security (encryption, authentication/segmentation, etc)

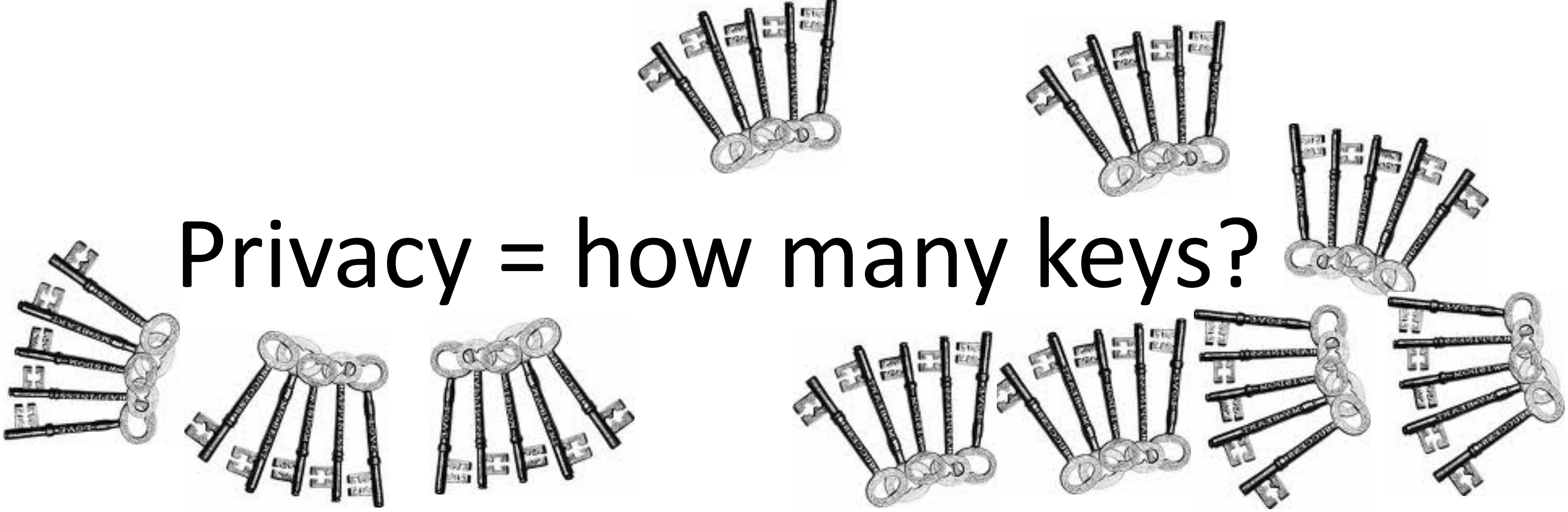
HITECH: consumer protections

Consumer Choices Technology Hearing

ideal HIT systems, VA?

security ≠ privacy

Privacy = how many keys?



Security

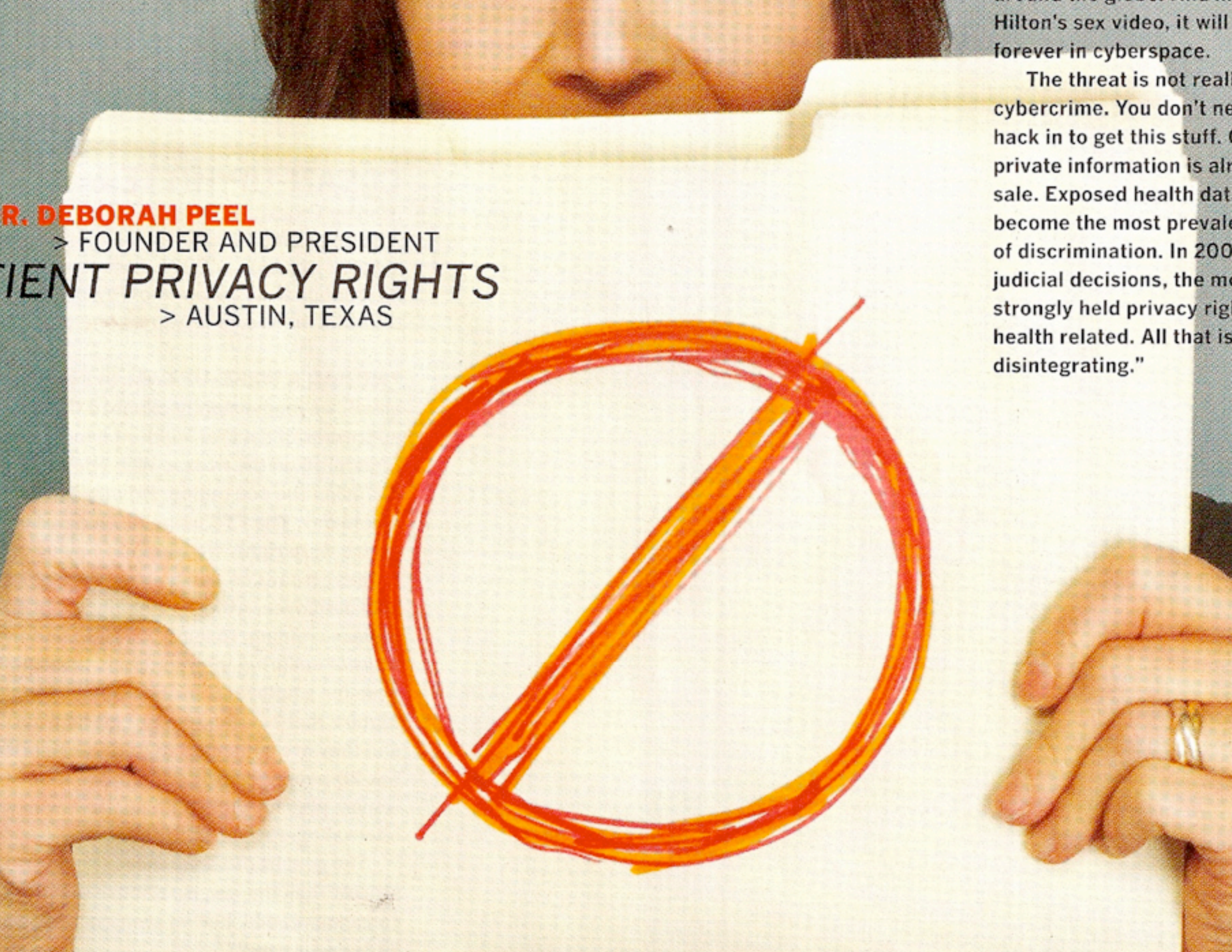
What does ‘privacy’ mean?

The *NCVHS* defined health information privacy as

“an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data”.

(June 2006, NCVHS Report to Sec. Leavitt, definition originally from the IOM) privacy = control

comprehensive and
meaningful
privacy
and security



R. DEBORAH PEEL
> FOUNDER AND PRESIDENT
IENT PRIVACY RIGHTS
> AUSTIN, TEXAS

Hilton's sex video, it will
forever in cyberspace.

The threat is not reall
cybercrime. You don't ne
hack in to get this stuff.
private information is alr
sale. Exposed health dat
become the most prevale
of discrimination. In 200
judicial decisions, the mo
strongly held privacy rig
health related. All that is
disintegrating."

10 Million Americans Expect Privacy and Security

The bipartisan Coalition for Patient Privacy, 2010

AIDS Action
American Association of People with Disabilities
American Association of Practicing Psychiatrists
American Chiropractic Association
American Civil Liberties Union
American Conservative Union
American Psychoanalytic Association
Association of American Physicians and Surgeons
Bazelon Center for Mental Health Law
Bob Barr (former Congressman R-GA)
Citizens for Health
Citizen Outreach Project
Clinical Social Work Association
Consumer Action
Consumers for Health Care Choices
Cyber Privacy Project
Doctors for Open Government
Ethics in Government Group
Fairfax County Privacy Council
Family Research Council
Free Congress Foundation
Georgians for Open Government
Gun Owners of America
Health Administration Responsibility Project, Inc.
Just Health
Multiracial Activist
Microsoft Corporation Inc.
National Center for Transgender Equality
The National Center for Mental Health Prof. & Consumers
National Whistleblower Center
National Workrights Institute
Natural Solutions Foundation
New Grady Coalition
Pain Relief Network
Patient Privacy Rights Foundation
Privacy Activism
Privacy Rights Now Coalition
Private Citizen, Inc.
Republican Liberty Caucus
Student Health Integrity Project
TexPIRG
Thoughtful House Center for Autism
Tolven, Inc.
Tradition, Family, Property, Inc.
Universata, Inc.
U.S. Bill of Rights Foundation
You Take Control, Inc.

clinical justification for security: patients’ expectations and rights

AHRQ: 2009
20 focus groups expect control

- A majority want to "own" their health data, and to decide what goes into and who has access to their medical records. (AHRQ p. 6)

- A majority believe their medical data is "no one else's business" and should not be shared

  without their permission….not about sensitive data but "a matter of principle". (AHRQ p. 18)

AHRQ: 2009
20 focus groups expect control

- no support for general rules that apply to all consumers

- consumers should exert control over their own health information **individually, rather than collectively**.(AHRQ p. 29)

AHRQ Publication No. 09-0081-EF “Final Report: Consumer Engagement in Developing Electronic Health Information Systems” Prepared by: Westat, (July 2009)

http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf

2006 Privacy and EHR Systems: Can We Avoid A Looming Conflict?

42% of public feels potential privacy ***risks outweigh*** potential EHR ***benefits***

60% of public wants to know EHR impacts and the ***right to choose*** how records used

http://patientprivacyrights.org/media-center/polls/#Electronic

Dr. Alan F. Westin
Professor of Public Law and
Government Emeritus, Columbia University

Markle Conference on "Connecting Americans to Their Health Care," Washington, D.C. Dec 7-8, 2006

2009 NPR/Kaiser/Harvard Poll

The Public and the Health Care Delivery System

59% are ***NOT confident*** online medical ***records will remain confidential***

76% believe ***unauthorized persons will access*** their online medical records

http://www.kff.org/kaiserpolls/upload/7888.pdf

The right of privacy is a personal and fundamental right in the United States

See Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 763 (1989) ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person"); *Whalen v. Roe*, 429 U.S. 589, 605 (1977); *United States v. Katz*, 389 U.S. 347 (1967); *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.

Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* 11 (2009) (charts describing how identity theft victims' information have been misused).

As the Supreme Court has made clear, and the DC Circuit Court of Appeals recently held, "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."

U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989), cited in *Nat'l Cable & Tele. Assn. v. Fed. Commc'ns. Comm'n*, No. 07-1312 (D.C. Cir. Feb. 13, 2009).

"the constitutionally protected right to privacy of highly personal information is so well established that no reasonable person could be unaware of it."

Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000).

ethical and human rights to privacy

legal privileges
common law

The Madrid Privacy Declaration of November 2009 affirms that **privacy is a <u>basic human right</u>**, and notes" corporations are acquiring vast amounts of personal data without independent oversight"

The Madrid Privacy Declaration: Global Privacy Standards for a Global World,

Nov. 3, 2009, *see* http://thepublicvoice.org/madrid-declaration/ .

Professional and research ethics

The ethical codes of all health professions require informed consent before use or disclosures of personal health information.

Report to HHS, NCVHS (June 22, 2006)

“the well- being of the human subject should take precedence over the needs and interests of society”

World Medical Association Declaration of Helsinki June 1964
Ethical Principles for Medical Research Involving Human Subjects

Privileges and Common Law

A physician-patient privilege is recognized in the laws of 43 states and the District of Columbia.

The State of Health Privacy, Health Privacy Project (2000)

All 50 states and the District of Columbia recognize in tort law a common law or statutory right to privacy of personal information.

HHS finding 65 Fed. Reg. at 82,464

Ten states have a right to privacy expressly recognized in their state constitutions.

loss of reputation/
liability:
ASU
TX Dept of Health

April 21, 2010

Indian Tribe Wins Fight to Limit Research of Its DNA

By AMY HARMON

http://www.nytimes.com/2010/04/22/us/22dna.html?ref=us

THE TEXAS TRIBUNE

DNA Deception

by Emily Ramshaw
February 22, 2010

“nine years' worth of e-mails and internal documents on the Department of State Health Services’ newborn blood screening program reveals the transfer of hundreds of infant blood spots to an Armed Forces lab to build a national and, someday, international mitochondrial DNA (mtDNA) registry” no support for research without consent

Westin/Harris Survey for the Institute of Medicine

Results of a National Survey
Commissioned by the IOM Committee on
“Health Research and the Privacy of
Health Information: The HIPAA Privacy Rule”

Original Report - November 2007; Revised and expanded - March 2008

IOM Survey: People Won’t Participate in Research Without Privacy

- Only 1% agreed that researchers would be free to use personal medical and health information without consent
- Only 19% agreed that personal medical and health information could be used as long as the study “never revealed my personal identity” and it was supervised by an Institutional Review Board.

http://patientprivacyrights.org/media/WestinIOMSrvyRept.pdf?docID=2501

research on consent for use of newborn bloodspots

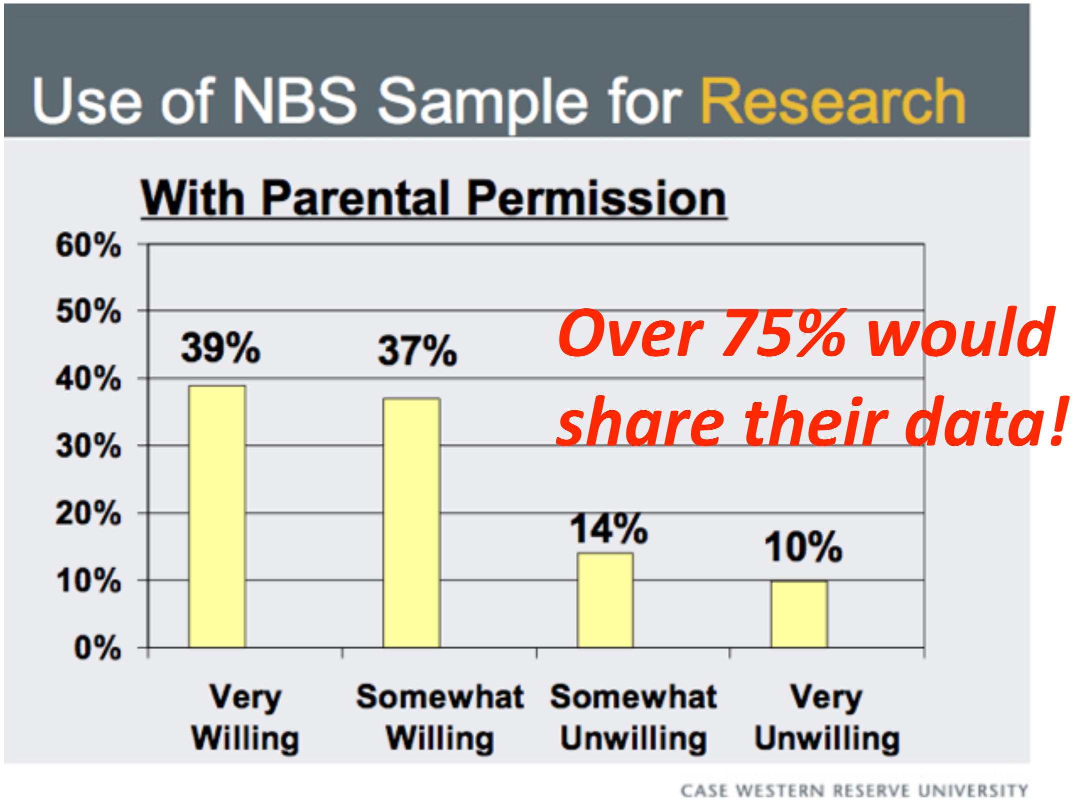
From Public Health Genomics

When Asked, Consumers Support Use of Their Data

"How willing are you to have your child's blood sample (from newborn screening) used for future research studies, with (or without) your permission?"

Four choices were:

- ***Very willing***
- ***Somewhat willing***
- ***Somewhat unwilling***
- ***Very unwilling***



Over 75% would share their data!

Source: Dr. Aaron Goldenberg (Case Western Reserve), *Public Health Genomics*, July 9, 2009 (as reported at Genetic Alliance Conference on Newborn Screening, December 2009).

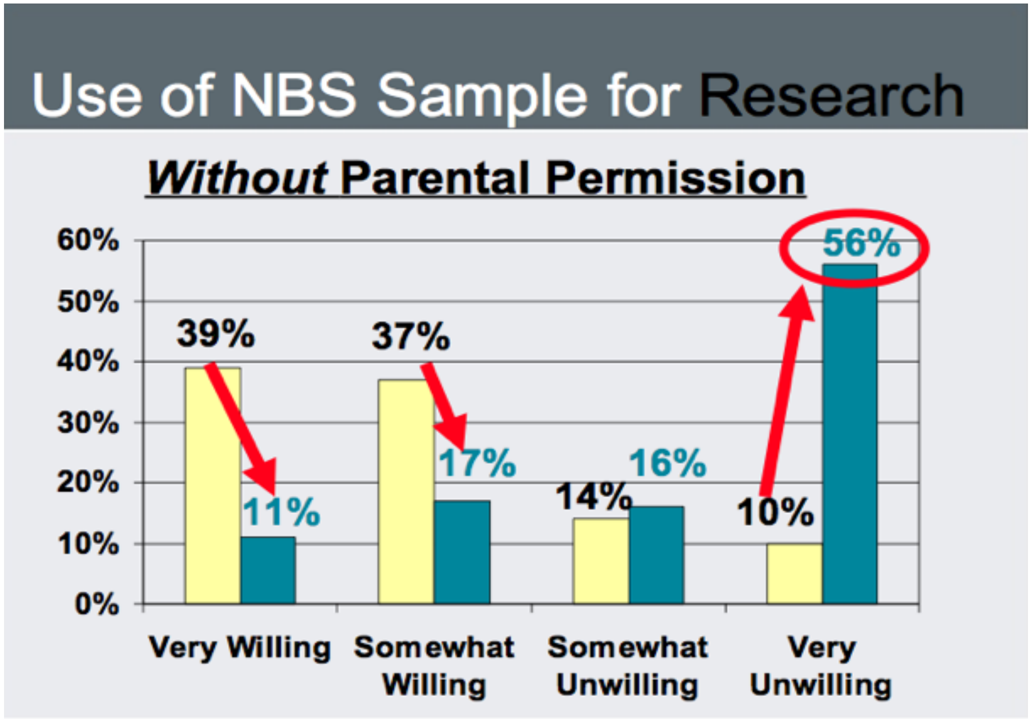
When ~~Asked~~ If, Consumers Support Use of Their Data

"How willing are you to have your child's blood sample (from newborn screening) used for future research studies, with (or without) your permission?” ***WITHOUT CONSENT Only 28% were OK with research***
use ***and 72% were NOT OK with research***

Four choices were:

- ***Very willing***
- ***Somewhat willing***
- ***Somewhat unwilling***
- ***Very unwilling***

Source: Dr. Aaron Goldenberg (Case Western Reserve), *Public Health Genomics*, July 9, 2009 (as reported at Genetic Alliance Conference on Newborn Screening, December 2009).



CASE WESTERN RESERVE UNIVERSITY

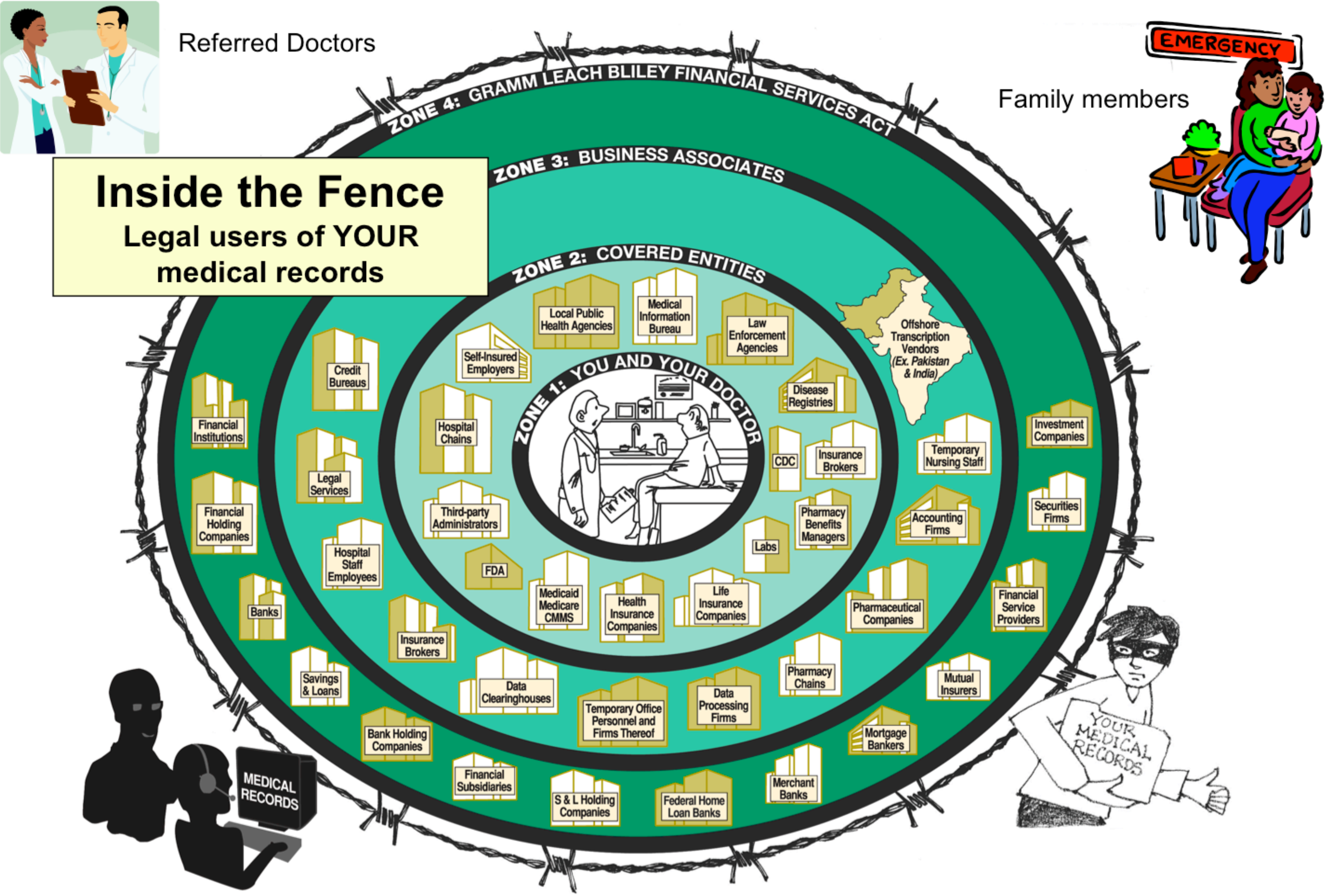
Americans expect privacy and control, but….

HIPAA regs eliminate consent and privacy

1996	Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HHS) was required to develop regulations that specified patients' rights to health privacy. **Public Law 104-191**	*"… the Secretary of Health and Human Services shall submit to [Congress]…**detailed recommendations on standards with respect to the privacy of individually identifiable health information."***
2001	President Bush implemented the HIPAA "Privacy Rule" which recognized the "right of consent". HHS wrote these regulations. **65 Fed. Reg. 82,462**	*"….a covered health care provider **must obtain the individual's consent,** in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations."*
2002	**HHS amended the HIPAA "Privacy Rule", eliminating the right of consent.** **67 Fed. Reg. 53,183**	*"The **consent provisions…are replaced** with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations."*

Inside the Fence

Legal users of YOUR medical records



www.patientprivacyrights.org

Americans expect privacy and security,

but....

Where did this slide come from ? The Medical Information Bureau website. The MBI sells claims/health data to insurers and employers.

35% of Fortune 500 companies admit to using medical records for hiring and promotions

65 Fed. Reg. 82,467.

huge market for health data

+

theft and sale of health data

health data mining industry

2010: Top Fortune 500 Companies health data mining industry

4 General Electric (GE Centricity EHR/HIT systems, ***sells clinical data***) revenue 157B

14 McKesson (***sells Rx data***) revenue 107B

18 CVS Caremark (***sells Rx data***) revenue 99B

21 UnitedHealth Group (***sells RX data*** thru Ingenix subsidiary) revenue 87B

31 WellPoint (***sells claims/clinical data*** via BHI) revenue 65B

http://money.cnn.com/magazines/fortune/fortune500/2010/full_list/

2010: Top Fortune 500 Health Care: Pharmacy and Other Services (health data mining industry)

Rank	Company/500 rank	Revenues($ billions)	
1	Medco Health Solutions #35	59.8	(sells Rx data)
2	HCA (largest US hospital chain) #77	30	(?? sells hospital and Rx data)
3	Express Scripts #96	25	(sells Rx data)
4	Quest Diagnostics #303 “transforms millions of test results into valuable information products” http://www.questdiagnostics.com/brand/careers/index.html#services	7	(sells data/sends data to HIEs?)
5	Omnicare #347 (leading Rx provider for seniors)“we capture a tremendous amount of data” ..combines data with outcomes algorithm technology	6.3	(???)
6	Lab Corp. of America #442	4.7	(sells data??/sends data to HIEs)

EHRs, PHRs, claims data, lab data, prescriptions, health searches, etc

Prime*Research* ***part of an*** EHR/ Practice Management Suite

Key Benefits for Physicians:

“Make clinical research participation a revenue source” -

ie, doctors sell access to their patients and patients’ records

GREENWAY HELPS PHYSICIANS SELL:

- “de-identified” clinical data
- “de-identified” financial data
- population data
- data **on 19 M patients**
- **8 million prescriptions/yr**
- data on **8,000 providers**

http://www.greenwaymedical.com/solutionprime-research/

The result – increased practice revenues and access to patient care improvements.”

athenahealth

athenahealth strives to be the best at getting doctors paid

used by **19,500 physicians and medical providers** nationwide

http://www.athenahealth.com/strategic-alliances/index.phphttp://www.athenahealth.com/strategic-alliances/index.php

Xconomy | Boston
Business + Technology in the Exponential Economy

Athenahealth Paying Dearly to Take on Larger Rivals

by Ryan McBride 5/6/10

Athena might be able to halve the amount that physicians pay to use its EHR if they participate in "AthenaCommunity."

Athena's EHR customers who opt to share their patients' data with other providers **would pay a discounted rate to use Athena's health record software**.

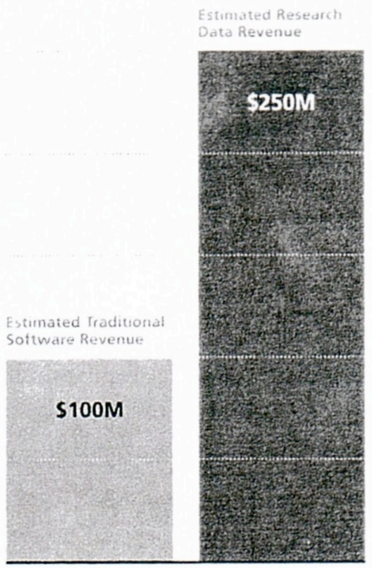
Athena would be able to make money with the patient data by charging, say, a hospital a small fee to access a patient's insurance and medical information from Athena's network.

http://www.xconomy.com/boston/2010/05/06/athenahealth-paying-dearly to-take-on-largerrivals/3/

HOW CAN HEALTHCARE SOFTWARE BE FREE?

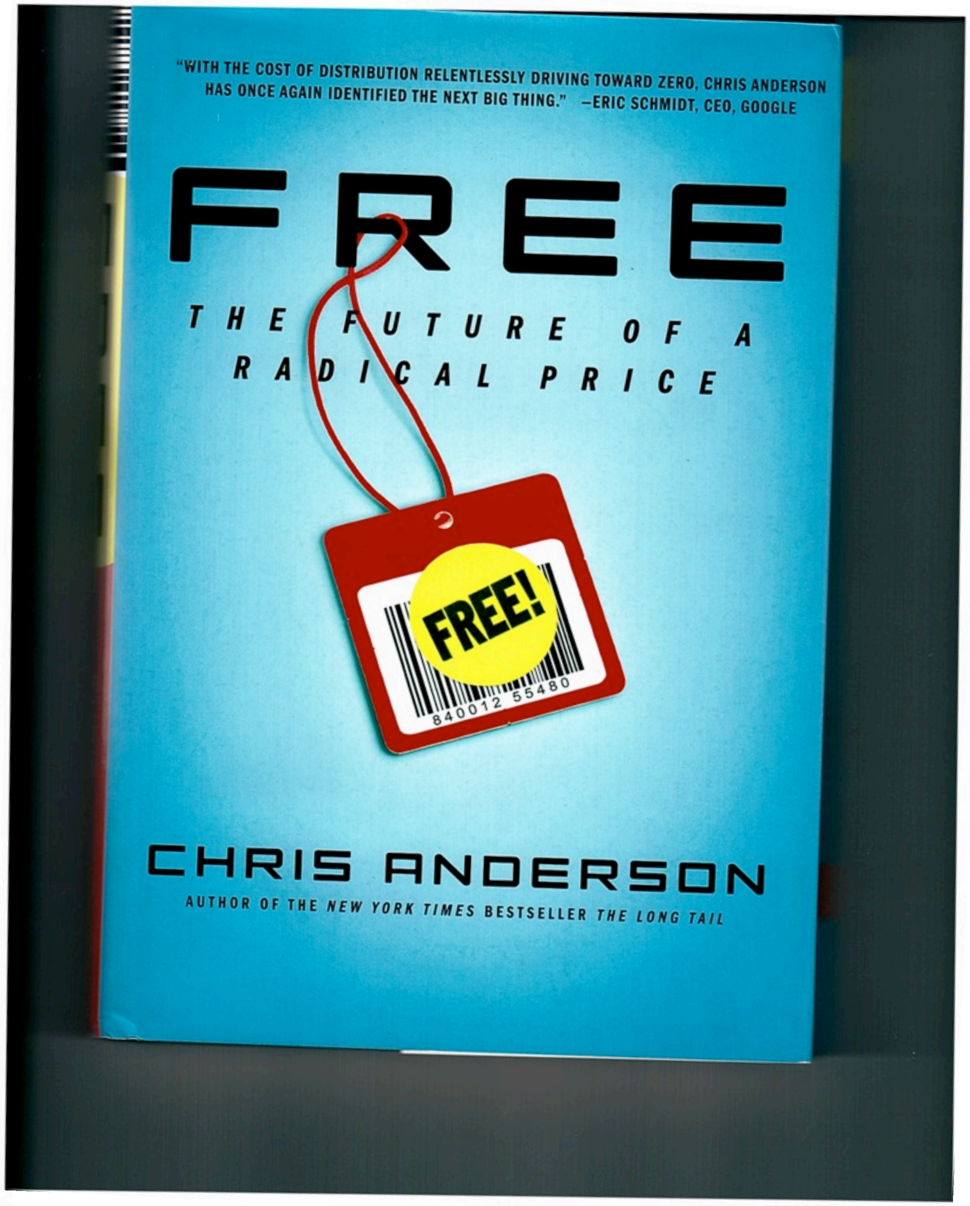
Since November 2007, thousands of physicians have signed up to receive free electronic health record and practice management software from San Francisco-based start-up Practice Fusion. Enterprise software for medical practices can cost $50,000. How can one company give away its e-record system at no charge?

Sellling data can be more profitable than selling software.



- **Freemium + advertising.** Tapping the freemium model, Practice Fusion offers two versions of its software: a free one that serves ads (à la Google AdSense), and an ad-free one that costs $100 per month. Of the first 2,000 doctors to adopt Practice Fusion's e-record system, less than 10 percent opted to pay. But the real revenue lies elsewhere...

- **Sell access to your data.** Using free software, Practice Fusion attracts a critical mass of users (doctors) who, in turn, create a growing database of patients. Medical associations conducting research on specific conditions require longitudinal health records for a large set of patients. Depending on the focus of a study (think: white, middle-aged, obese males suffering from asthma), each patient's anonymized chart could fetch anywhere from $50 to $500. A physician typically sees about 250 patients, so Practice Fusion's first 2,000 clients translates to 500,000 records. Each chart can be sold multiple times for any number of studies being conducted by various institutions. If each chart generates $500 over time, that revenue would be greater than if Practice Fusion sold the same 2,000 practices software for a one-time fee of $50,000.



Healthcare IT News

By Diana Manos, Senior Editor
12/31/07

Practice Fusion expands, shows signs of rapid growth

Practice Fusion subsidizes its free EMRs by selling de-identified data to insurance groups, clinical researchers and pharmaceutical companies.

Howard said he does not expect data-sharing will be a concern to physicians who use Practice Fusion's EMRs. ***"Every healthcare vendor is selling data."***

What is BHI® (Blue Health Intelligence)?

shares critical health information with employers
premier health intelligence resource
BHI sets the new standard for healthcare data aggregation, reporting and analysis

Size and Value of data for sale

1) **longitudinal data on 54 million BCBS members** [without consent]
2) reporting not only by MSA, industry and product type, but by ***Diagnosis Related Groups (DRGs)*** code, ***age group*** and ***gender*** [allows re-identification]

How does BHI ensure the privacy and security of members' healthcare information?

1) **adheres to HIPAA regs** = no consent for use and sale of data
2) Use a *system-generated identifier,* allowing *longitudinal analysis* [allows re-identification]
3) **fully de-identified in accordance with HIPAA** [17 identifiers removed, still allows re-identification of .04%]

http://www.bcbs.com/innovations/bhi/bhi-faqs-1-12-09.pdf

Medicare and Medicaid data for sale “at the patient level”

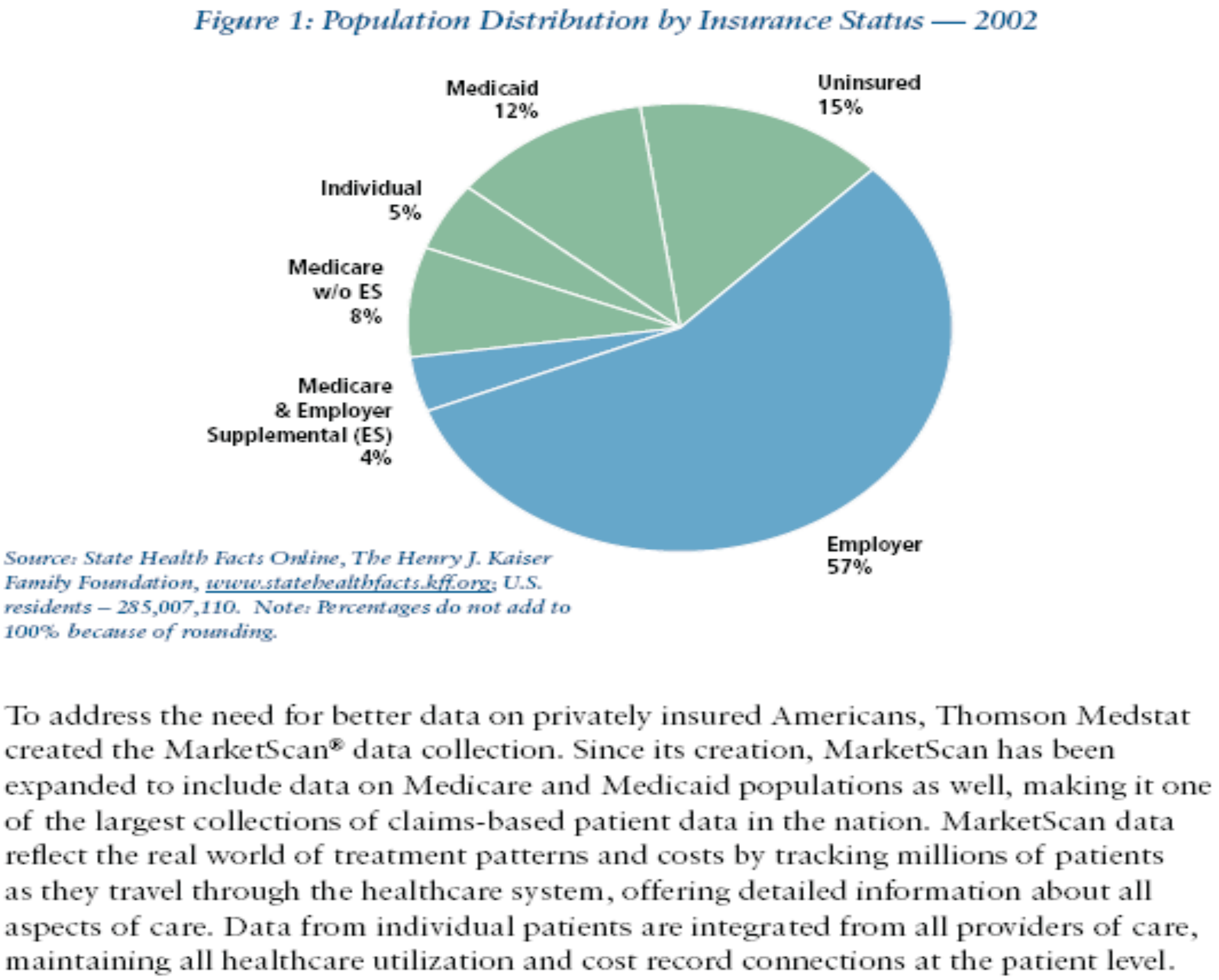
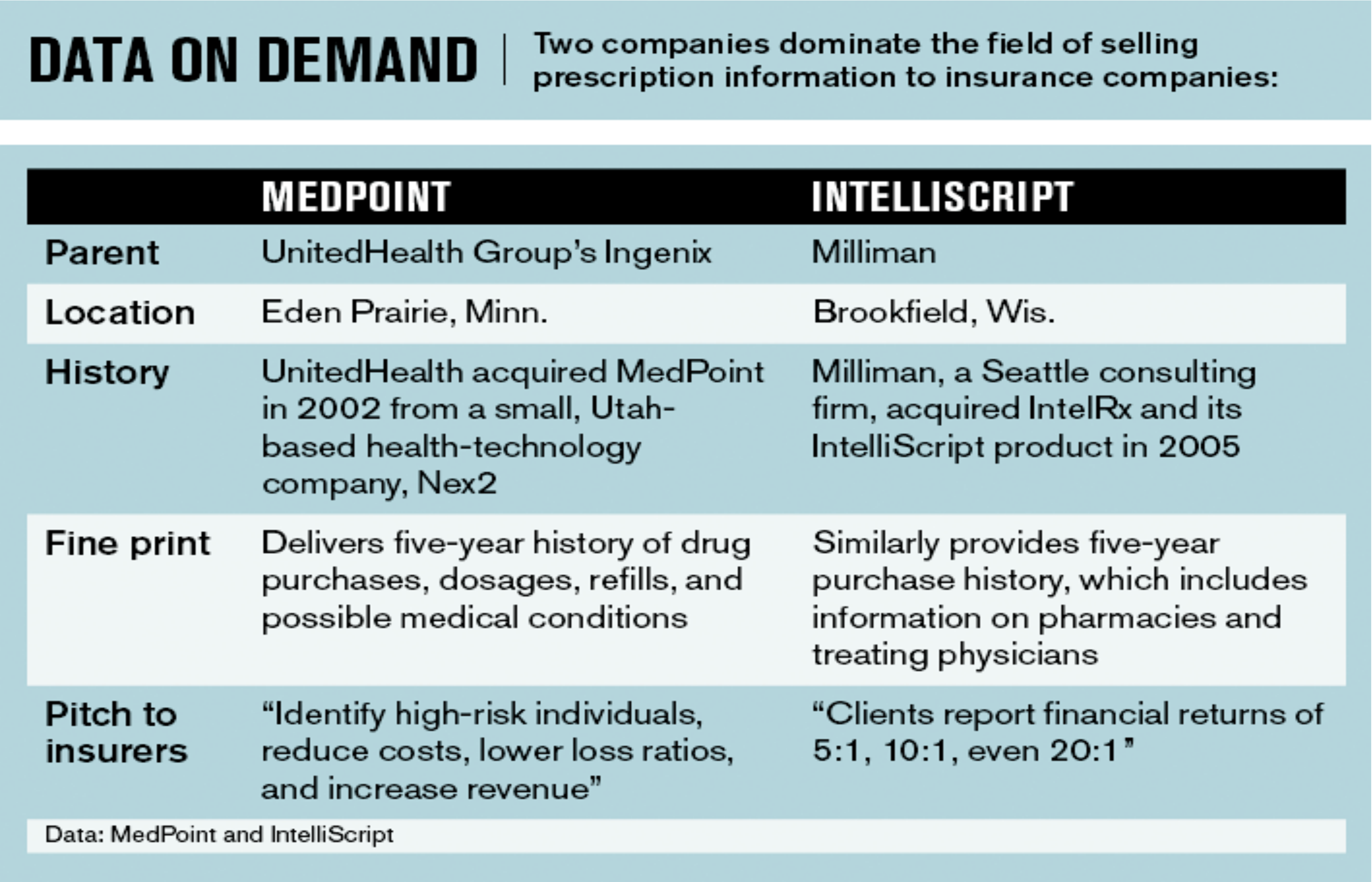


Figure 1: Population Distribution by Insurance Status — 2002

Source: State Health Facts Online, The Henry J. Kaiser Family Foundation, www.statehealthfacts.kff.org; U.S. residents – 285,007,110. Note: Percentages do not add to 100% because of rounding.

To address the need for better data on privately insured Americans, Thomson Medstat created the MarketScan® data collection. Since its creation, MarketScan has been expanded to include data on Medicare and Medicaid populations as well, making it one of the largest collections of claims-based patient data in the nation. MarketScan data reflect the real world of treatment patterns and costs by tracking millions of patients as they travel through the healthcare system, offering detailed information about all aspects of care. Data from individual patients are integrated from all providers of care, maintaining all healthcare utilization and cost record connections at the patient level.

Businessweek July 23, 2008: *“They Know What's in Your Medicine Cabinet, How insurance companies dig up applicants' prescriptions—and use them to deny coverage"* http://www.businessweek.com/magazine/content/08_31/b4094000643943.htm?chan=magazine+channel_in+depth



DATA ON DEMAND | Two companies dominate the field of selling prescription information to insurance companies:

	MEDPOINT	INTELLISCRIPT
Parent	UnitedHealth Group's Ingenix	Milliman
Location	Eden Prairie, Minn.	Brookfield, Wis.
History	UnitedHealth acquired MedPoint in 2002 from a small, Utah-based health-technology company, Nex2	Milliman, a Seattle consulting firm, acquired IntelRx and its IntelliScript product in 2005
Fine print	Delivers five-year history of drug purchases, dosages, refills, and possible medical conditions	Similarly provides five-year purchase history, which includes information on pharmacies and treating physicians
Pitch to insurers	“Identify high-risk individuals, reduce costs, lower loss ratios, and increase revenue”	“Clients report financial returns of 5:1, 10:1, even 20:1”

Data: MedPoint and IntelliScript


TAKE YOUR
HEALTH DATA
"OFF THE MARKET".
watch the video ▶
VIAGRA
FOR
ERECTILE
DYSFUNCTION
CAMPAIGN for
PRESCRIPTION
PRIVACY

HITECH:
historic new consumer protections, but…

ARRA—new privacy rights and MU

Old rights under HIPAA:

- Providers may offer consent (Original HIPAA Privacy Rule), so patients can restrict disclosures---not addressed in MU
- Psychotherapy Notes require consent to disclose---not addressed in MU

New rights under ARRA:

- Ban on sales of PHI (Protected Health Information)---2010 (waiting for comments on NPR and final rule)
- Segmentation---delayed
- Audit trails x 3 years---2011 or later
- Breach notice---2010 (added "harm" standard violates HITECH!)
- Encryption---2010 but industry is not doing this
- Patient can prevent disclosures of PHI for 'payment and healthcare operations' if pays out-of-pocket---not addressed
- Consent Technologies---2014 or later

“Meaningful Use”
isn’t meaningful to
patients

Latanya Sweeney on flaws in MU EHR criteria and NHIN/HIEs

Secondary use of PHI by Business Associates is "unbounded, widespread, hidden, and difficult to trace."

Implementing **MU EHRs will "increase data sharing, but adding the NHIN will massively increase data sharing."**

The two proposed NHIN models to link all Americans' health information online do not offer "utility or privacy".

http://patientprivacyrights.org/wp-content/uploads/2010/04/Sweeney-CongressTestimony-4-22-10.pdf

Sweeney on designing privacy in HIT

Observation: "Scott McNealy, the CEO of Sun Microsystems, famously quipped, "**Privacy is dead. Get over it**."

Sweeney's response: "Oh privacy is definitely not dead. ***When people say you have to choose, it means they haven't actually thought the problem through or they aren't willing to accept the answer***.

… ***he very much shares that attitude of the computer scientist who built the technology that's invasive; who says, "Well, you want the benefits of my technology, you'll get over privacy".***

It's exactly the kind of computer scientist we don't want to be graduating in the future.”

http://patientprivacyrights.org/2007/06/privacy-isnt-dead-or-at-least-it-shouldnt-be-a-qa-with-latanya sweeney

MU EHR flaws

- data mining for many uses without informed consent
- "unbounded uses" by CEs and BAs—no trust without verification

NHIN/RHIO/HIE/HIO flaws

- allow broad "stakeholder" (insurers, employers) access to data
- patients don't want "stakeholder" access, they want control
- impossible to share data selectively (segment sensitive records)
- illegal, blanket consents = impossible to share data 1-to-1
- labs and Rx data industry will dump 1,000s of "batched" test reports and prescriptions into HIOs—patients' privacy will be violated even if they opt-out
- without segmentation, HIE/NHIN can't exchange data across state lines with states---all states require consent for sensitive data (segmentation)
- without segmentation can't put teens' data, genetic data, STDs, mental health, addiction data into HIT systems

54 " Tall

54 " Tall

54 " Tall

Health IT and HIE: 2 separate worlds

Corporations, Govt, & some Doctors

- **Industry-centered system**
- LOTS of Data = commodity = $$$$
- massive data flows and 2ndary use of sensitive personal data
- Data theft, no consent
- Robust HIT systems
  - One hospital = 200+ HIT systems
- Robust HIE
- Vendors and users sell data
- Data flows outside US
- Massive security flaws
- “Wild West”-- data mining for profit and discrimination
- Unfair and deceptive trade practices

Patients, Family, & some Doctors:

- **Not “patient-centered”**
- Hardly any data
- Limited control over PHI
- Limited access to PHI
- Limited benefits from HIT
- Limited HIE
- Massive harms/risks from HIT/HIE
- Limited recourse from harms
- Can’t restore data privacy = no way to “make whole” or repair exposure
- Generations of discrimination
- Secret health data bases
- No transparency/accountability
- No privacy and weak security
- Patient Safety—EHRs can harm, be source of errors, can’t delete/amend

Will we finally get meaningful and comprehensive privacy and security?

Consumer Choices Technology Hearing

7 privacy-enhancing technologies 'live' demonstrations

Washington DC, June 29, 2010

video: http://nmr.rampard.com/hit/20100629/default.html

transcript and written testimony:

http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910

federal privacy precedents

- TITLE 38 - PART V , CHAPTER 73 - SUBCHAPTER III - PROTECTION OF PATIENTRIGHTS

  § 7332. (a) (1) **Confidentiality of certain medical records:** drug abuse, alcoholism or alcohol abuse, HIV, sickle cell anemia
- 42 CFR Part 2 alcohol and substance abuse

July 8, 2010 ***New*** Privacy Policy:

Sec. Sebelius: "Administration-wide commitment to make sure no one has access to your personal information unless you want them to”.

Dr. Blumenthal: "we want to make sure it is possible for patients to have maximal control over PHI."

See: http://patientprivacyrights.org/2010/07/ppr-impressed-with-hhs-privacy-approach/

Patient-centered HIT systems

1. universal online consent tools--benefits
   - dynamic, not static
   - fine-grained decisions, like online banking "Bill Pay"
     -automatic rules (like monthly payments), or case-by-case
   - ability to share selectively (in accord with laws, rights, expectations)
   - no need to update consents in many locations
   - no need for MPI or single patient ID
   - independent audit trails of all uses and disclosures via use of authentication and authorization systems
     (employees have unique access codes and can see selected data)

Your solution for controlling who sees your personal health information

Hello **Cassandra Hoag** (Sign Out)

View within: Past 3 years

Rotate Clockwise (Shift + Plus)

Rotate Counderclockwise (Shift + Minus)

Zoom In (Cntrl + Plus)

Zoom In (Cntrl + Minus)

Allow All

Allow None

Allow Selected

⚠ **Req. Attention**

Pref. Not Set
(e.g., Defaults to applicable Federal or state law)

© 2007 Private Access, LLC Legal Notices | Terms of Use | Privacy

Patient-centered HIT system

2. health banks--benefits
   - ironclad security and architecture
   - today there is no place w/ a complete and accurate copy of our health records
   - patients control access and use of PHI
   - ***only*** patients can collect complete and <u>accurate</u> PHI
   - ‘safer’ research, less risk of exposing data
     - like census bureau: run research queries on individual data
     - unlike census bureau, **no research without consent**
     - sensitive data is NOT released
   - no need for MPI or UPIN (single ID)---patients have separate ID at each location = better privacy protections (stolen data has less value)

Patient-centered HIT systems

3. other systems--benefits

- decentralized consents with centralized control. In this situation, patients can make local data sharing decisions at the time and place of service, but have a universal portal to update or change consents as needed

- an NHIN that works likes a filing cabinet. In this situation, all patient information goes to a common location, and the patient can make decisions about sharing at that storage location

Will the VA lead?

Deborah C. Peel, MD
Founder and Chair
(O) 512-732-0033

dpeelmd@patientprivacyrights.org

www.patientprivacyrights.org

patientprivacyrights

Key References:

EHRs “Your Medical Records Aren't Secure” *by Deborah C. Peel* in the WSJ, March 23, 2010 http://online.wsj.com/article/SB10001424052748703580904575132111888664060.html

PHRs “Who can snoop in your PHR? A Personal Health Record Report Card http://patientprivacyrights.org/personal-health-records/

HIEs and NHIN “Designing a Trustworthy Nationwide Health Information Network (NHIN) Promises Americans Privacy and Utility, Rather than Falsely Choosing Between Privacy or Utility” *by Latanya Sweeney, PhD,* April 22, 2010, Congressional Briefing on the “Implementation of Health Information Technologies in a Healthcare Environment”
http://patientprivacyrights.org/wpcontent/uploads/2101/04/SweeneyCongressTestimony-4-22-10.pdf

See Sweeney’s NHIN slides at:
http://patientprivacyrights.org/wp-content/uploads/2010/06/Sweeney TrustworthyNHINDesigns.pdf

Research “Improve Privacy in Research by Eliminating Informed Consent?” IOM Report Misses the Mark. In The Journal of Law, Medicine & Ethics, Volume 37, Issue 3 (p 507-512) *by Mark A. Rothstein. See: http://patientprivacyrights.org/library/ scroll down to Reports/ Studies*

Key References:

Patient-centric health care: “What Patient-Centered Should Mean: Confessions of An Extremist” *by Donald M. Berwick*, May 19, 2009 See: http://patientprivacyrights.org/library/ scroll down to More

Coalition for Patient Privacy: Comments of NPRM (changes to HIPAA) See: http://patientprivacyrights.org/2010/09/coalition-urges-hhs-to-restore-patient-control-over-access-to-health-data-now/

Anonymous data *isn't*

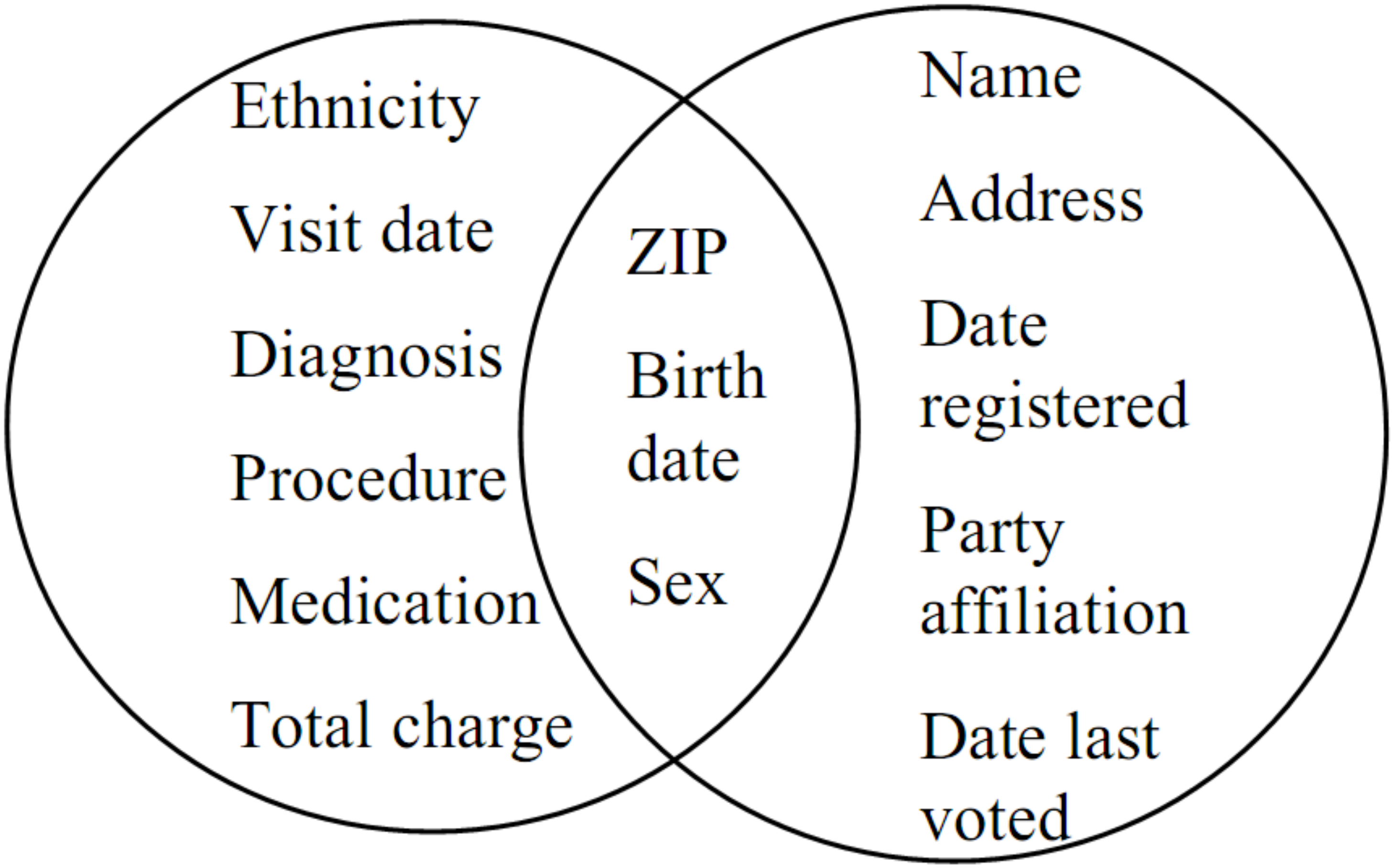
"… a common practice is for organizations to release and receive person specific data with all explicit identifiers, such as name, address and telephone number, removed ….because the resulting data look anonymous.

However,… the remaining data can be used to re-identify individuals by linking or matching the data to other data ..."*

Latanya Sweeney, PhD, Director, Laboratory for International Data Privacy, School of Computer Science, Carnegie Mellon University

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

Linking to re-identify data



Ethnicity

Visit date

Diagnosis

Procedure

Medication

Total charge

ZIP

Birth date

Sex

Name

Address

Date registered

Party affiliation

Date last voted

Medical Data **Voter List**

L. Sweeney. Weaving technology and policy together to maintain confidentiality. *Journal of Law, Medicine and Ethics*. 1997, 25:98-110.

Anonymous data *isn't*

"We must respond to the surprising failure of anonymization"

"Anonymization, [is] the name for techniques for protecting the privacy of individuals in large databases by deleting information like names and social security numbers"

"Scientists have demonstrated they can often "reidentify" or "deanonymize" individuals hidden in anonymized data with astonishing ease"*

Paul Ohm, Associate Professor, University of Colorado Law School

***** Broken promises of Privacy: Responding to the Surprising Failure of Anonymization, VER. 0.99 SSRN: 8/14/2009:

***http://**papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006&rec=1&srcabs=1446862*