WISE 2010: Women’s Institute in Summer Enrichment

the Team for Research in Ubiquitous Secure Technology (TRUST)

Healthcare, Health IT, and Health Information Exchange what do patients expect?

June 23, 2010

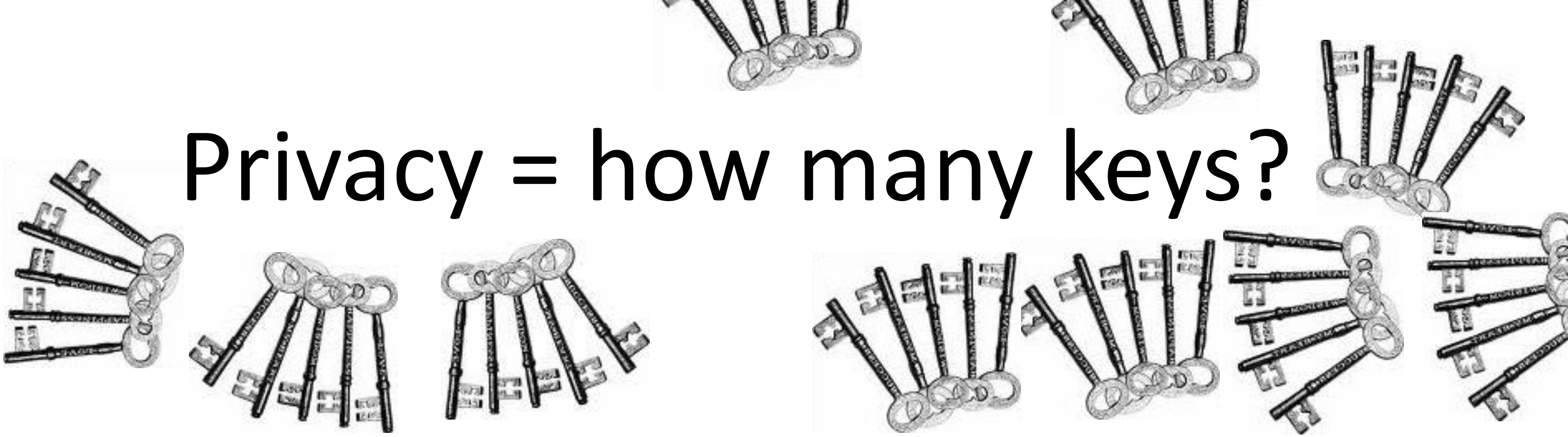
Deborah C. Peel, MD

patientprivacyrights

privacy and security
patients’ expectations/rights
HIPAA
other federal and state statutes
international framework (FIPS)
HITECH/ARRA
health data mining industry
liability/reputation
ideal HIT systems

privacy ≠ security

Privacy = how many keys?



Security

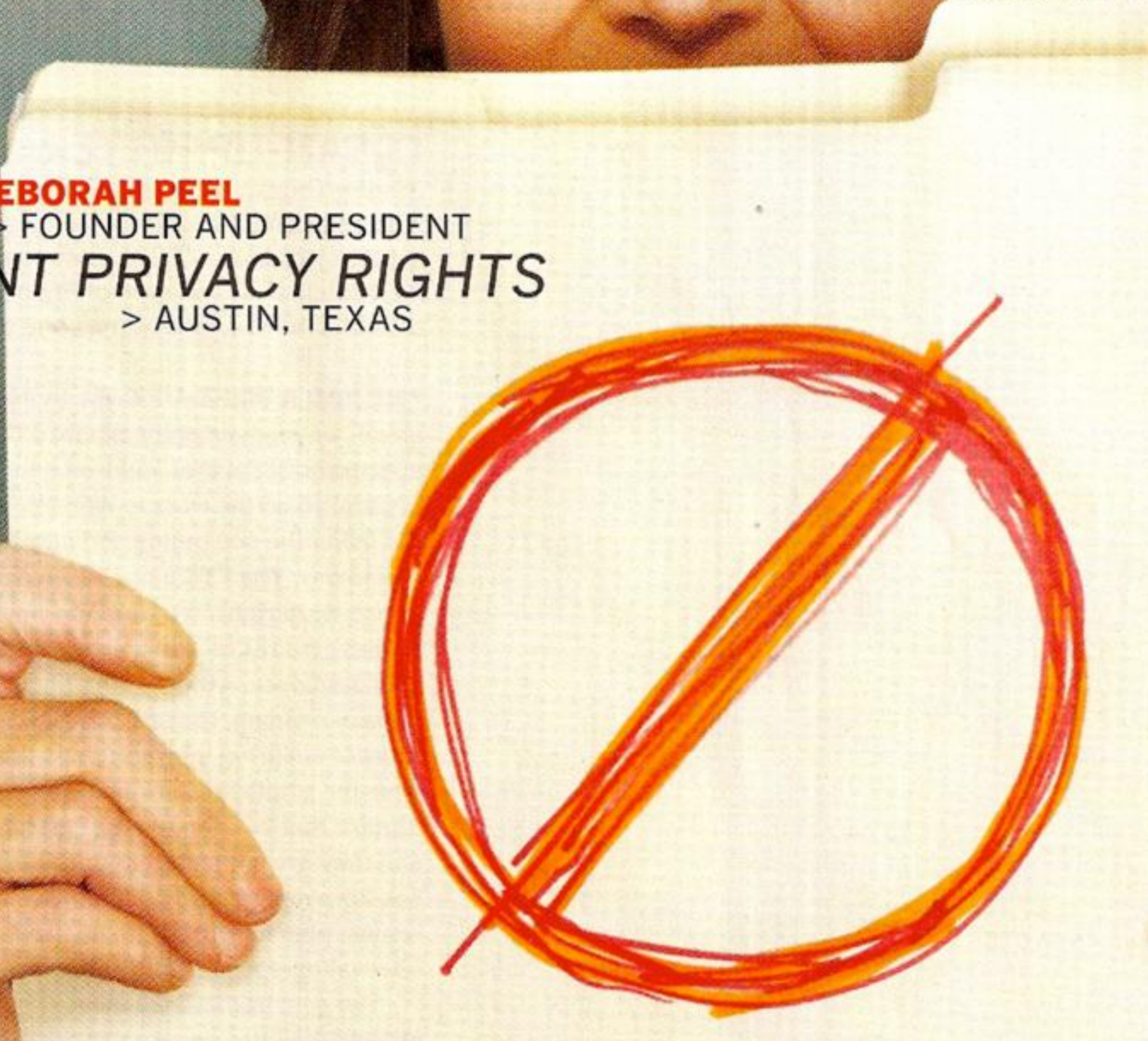
What does ‘privacy’ mean?

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



EBORAH PEEL
FOUNDER AND PRESIDENT
NT PRIVACY RIGHTS
> AUSTIN, TEXAS

The threat is no
cybercrime. You de
hack in to get this
private informatio
sale. Exposed heal
become the most p
of discrimination.
judicial decisions,
strongly held priva
health related. All
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.***

patients’ rights & expectations


MY WAY
WAY

AHRQ: 2009
20 focus groups expect control

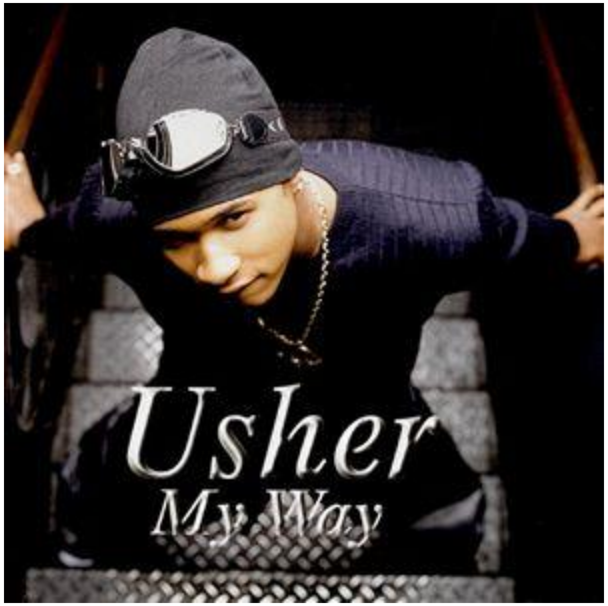
- A majority want to “own” their health data, and to decide what goes into and who has access to their medical records. (AHRQ p. 6)

- 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)


STEREO
MY WAY
FRAN

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)

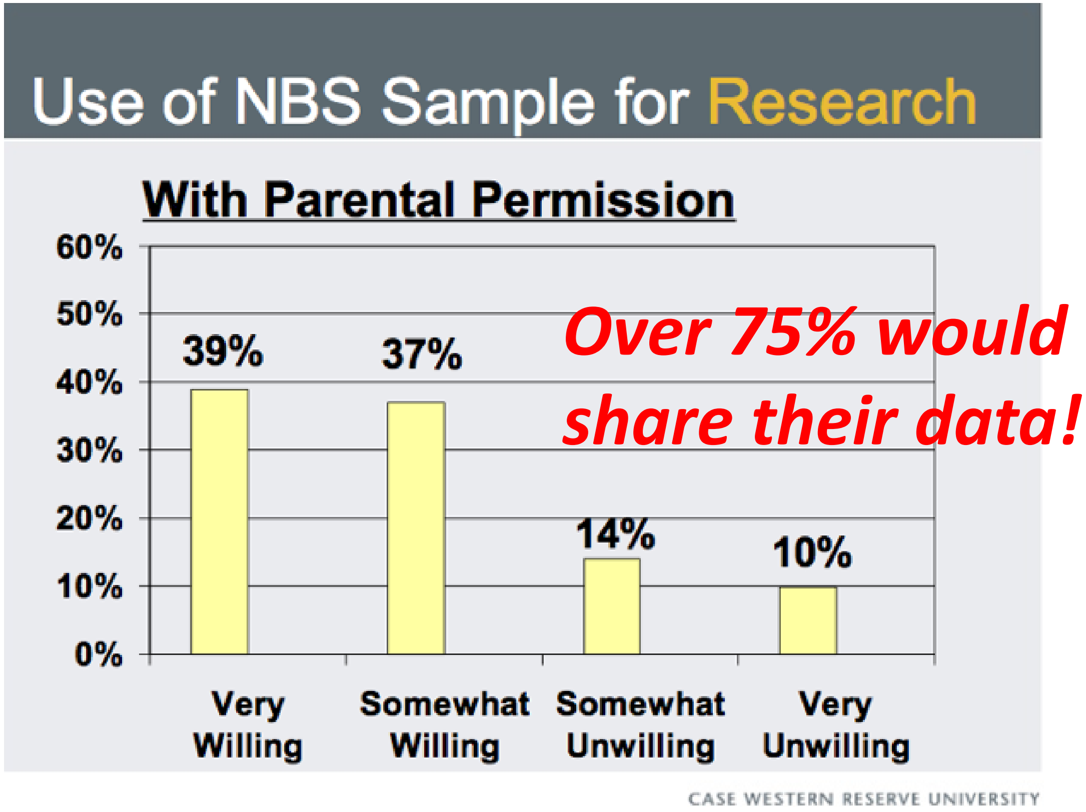
http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf

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).

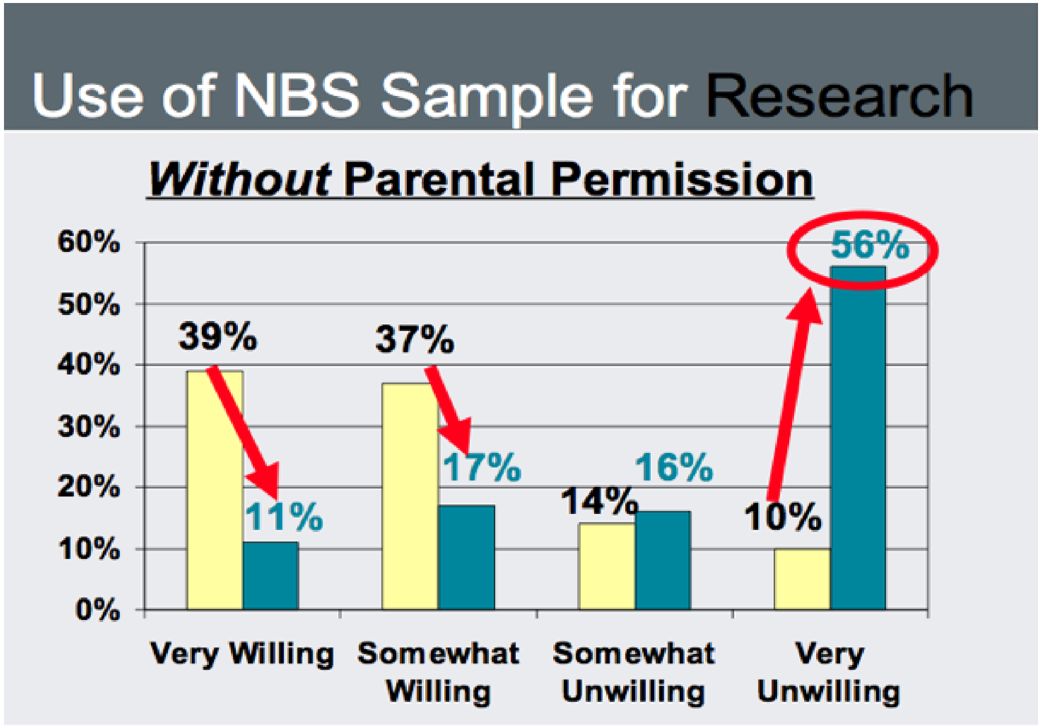
When ~~Asked~~ If, Consumers Support Use of Their Data

"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***



CASE WESTERN RESERVE UNIVERSITY

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

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

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

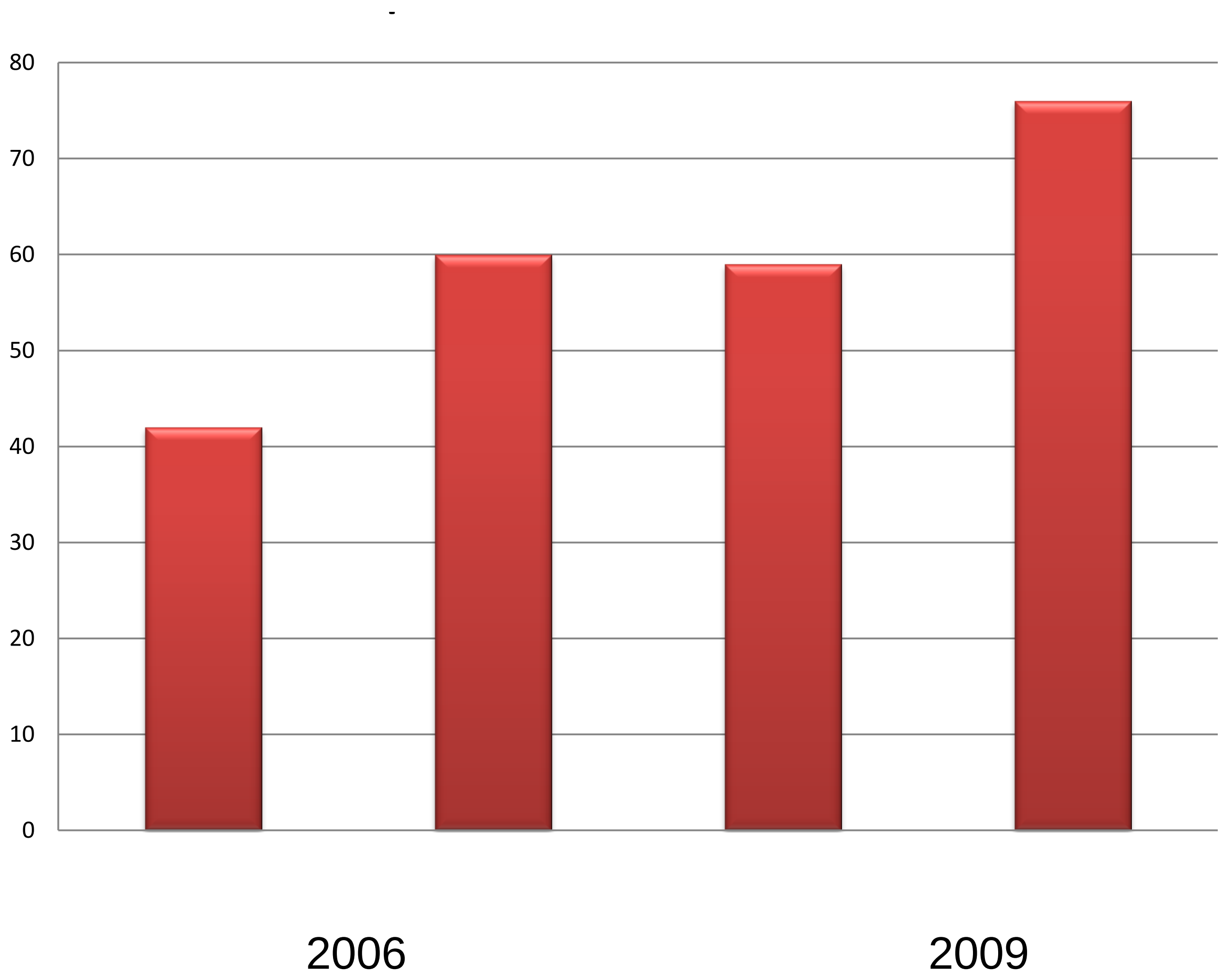
The Public and the Health Care Delivery System

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

public’s fears ↑↑↑



Americans expect privacy and control

but....

HIPAA was gutted in 2002

HIPAA regs eliminated consent and privacy

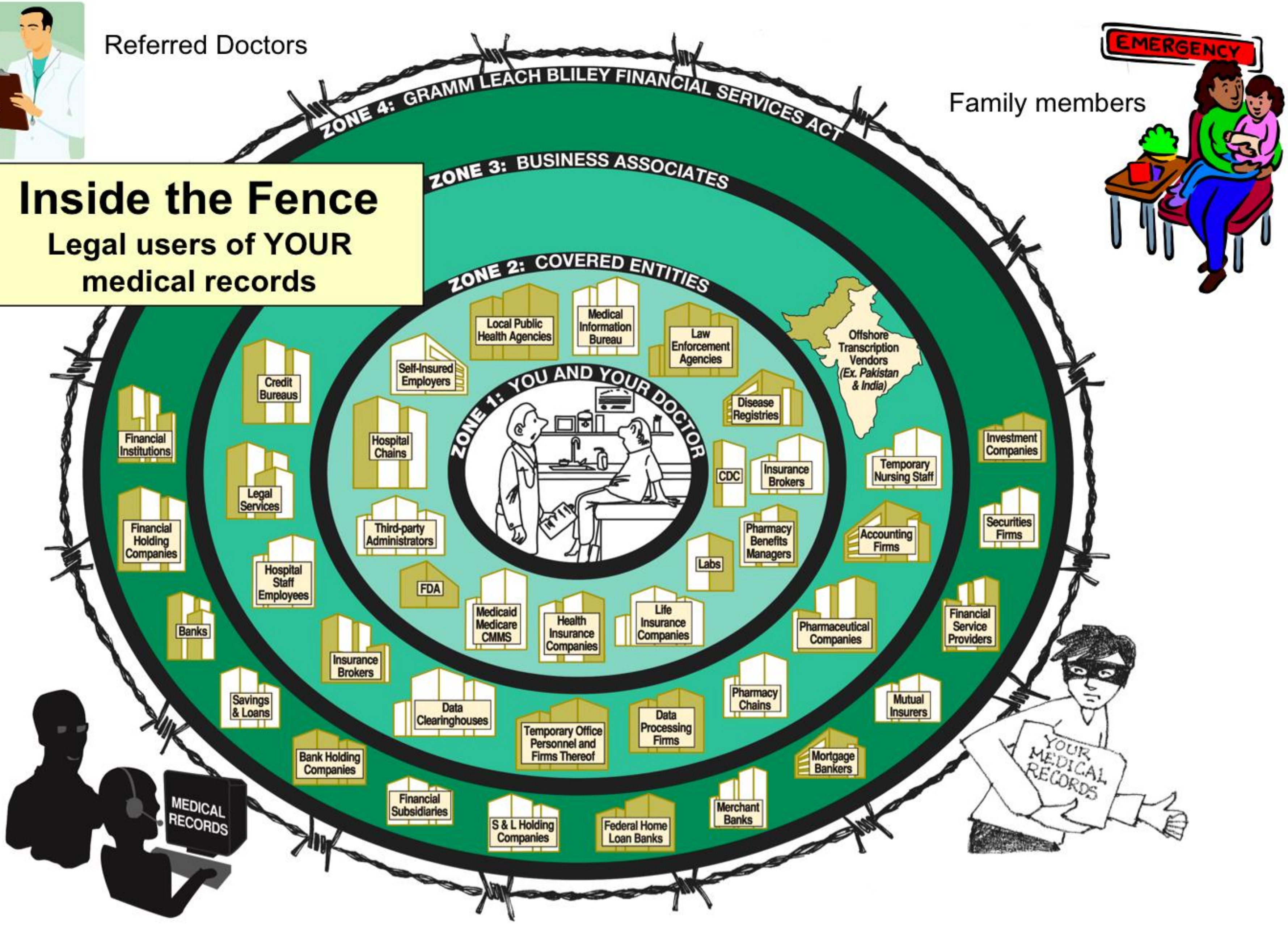
1996	Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HHS) was required to develop regulations that specified patients' rights to health privacy. **Public Law 104-191**	*"… the Secretary of Health and Human Services shall submit to [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."*

Referred Doctors

Family members

Inside the Fence

Legal users of YOUR medical records



www.patientprivacyrights.org

constitutional rights

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).

other

federal and state statutes

Other Key Federal rights

- 42 CFR Part 2---federal law requiring informed consent for the disclosure of alcohol and substance abuse treatment records
- HIPAA--- providers may offer a consent process, so there must be a way to provide informed consent for disclosures, and ‘psychotherapy notes’ must be segmented and require specific consent for disclosure

ethical and human rights to privacy

legal privileges
common law

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.

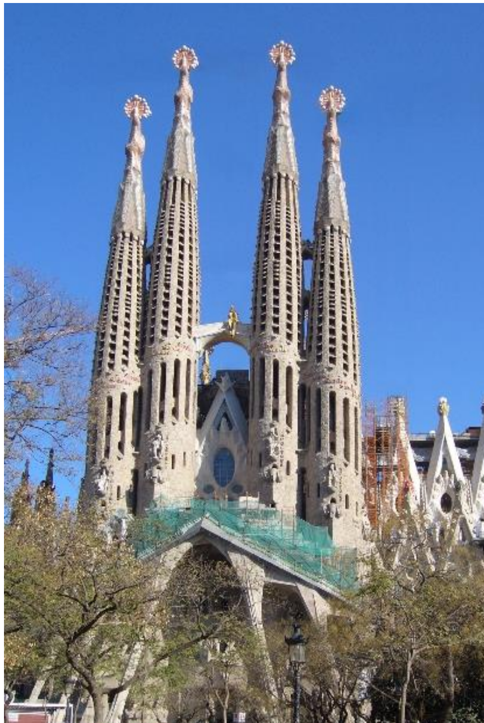
HHS finding 65 Fed. Reg. at 82,464

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

international frameworks
&
code of fair information practices (FIPS)

The Madrid Privacy Declaration of November 2009 affirms that **privacy is a basic human right**, 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/ .



The Code of Fair Information Practices

- There must be no personal data record-keeping systems whose very existence is secret = NO SECRET DATA BASES, limitation on collection
- There must be a way for a person to find out what information about the person is in a record and how it is used = transparency and disclosure
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent = single use
- There must be a way for a person to correct or amend a record of identifiable information about the person = right to correct errors
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. = data integrity, security, and accountability

U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973)

HITECH/ARRA: 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 NPR)
- Segmentation---delayed
- Audit trails x 3 years---2011 or later
- Breach notice---2010
- 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

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

“meaningful use” EHRs

no meaningful consent → “unbounded uses and disclosures” by CEs/BAs

NHIN/RHIOs/HIEs/HIOs

- “stakeholders” (insurers, employers) use data without consent
- patients don’t trust “stakeholders”
- patients can’t 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’ can’t opt-out
- without segmentation, can’t exchange data across state lines
- without segmentation, can’t put teens’ data, genetic data, STDs, mental health, addiction data into HIT systems

Americans expect privacy and security,

but....

huge market for health data

+

theft and sale of health data

health data mining industry

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

Wal-Mart Memo Suggests Ways to Cut Employee Benefit Costs

“Redesign benefits and other aspects of the Associate experience, such as job design, to attract a healthier, more productive workforce.”

“The team is also considering additional initiatives to support this objective, including: all jobs to include some physical activity (e.g., all cashiers do some cart gathering).”   October 26, 2005

The New York Times

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)

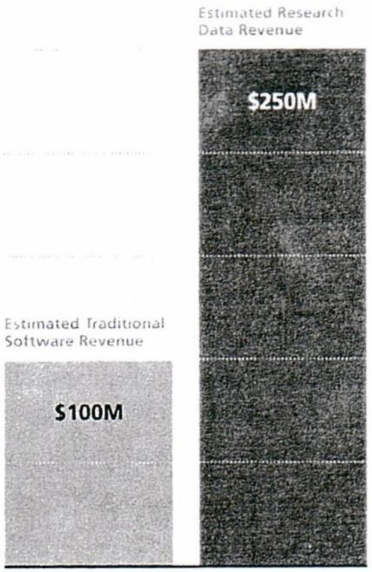
Rank	Company/500 rank	Revenues($ billions)	
1	Medco Health Solutions #35	59.8	(sells Rx data)
2	HCA (largest US hospital chain) #77	30	(?? sells hospital and Rx data)
3	Express Scripts #96	25	(sells Rx data)
4	Quest Diagnostics #303 "transforms millions of test results into valuable information products" 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

HOW CAN HEALTHCARE SOFTWARE BE FREE?

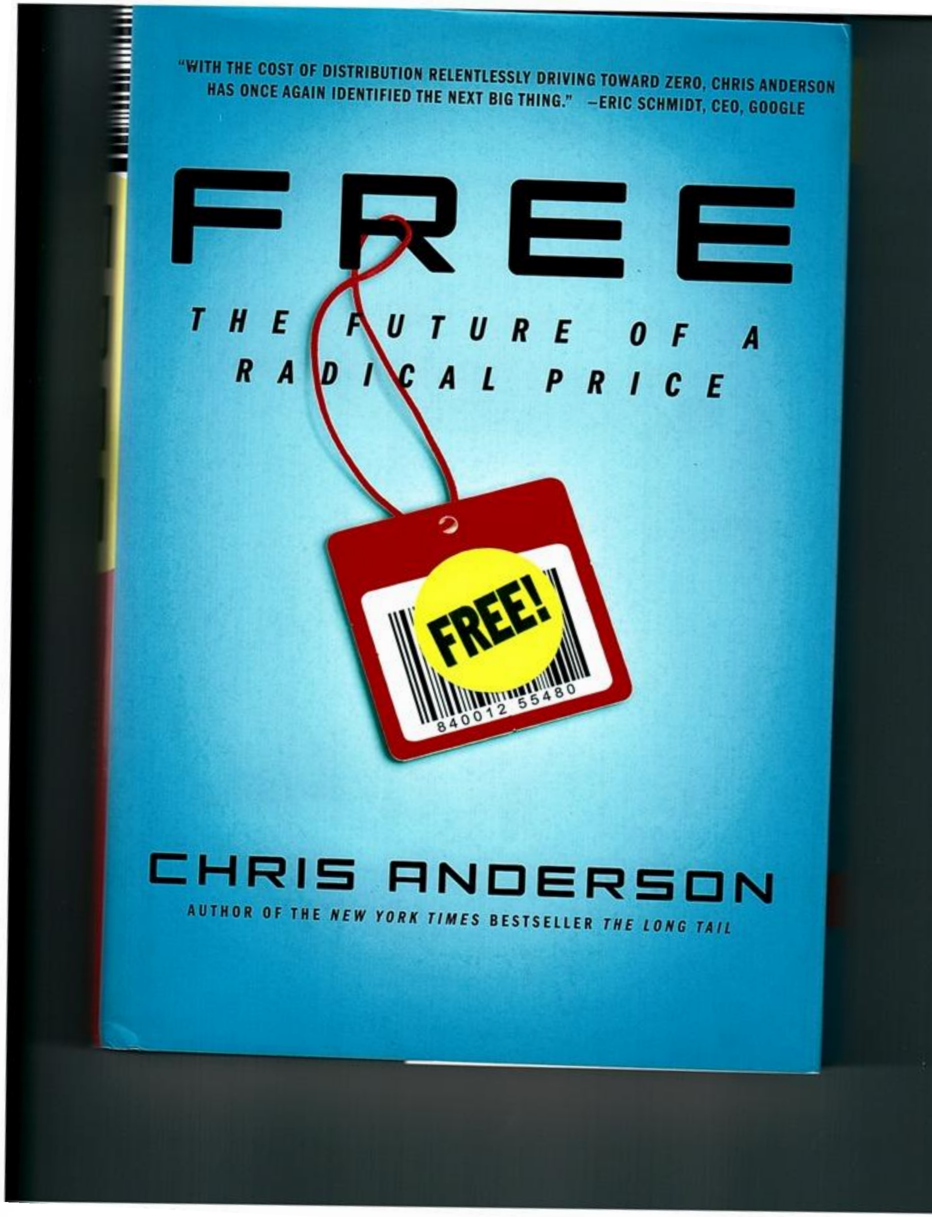
Since November 2007, thousands of physicians have signed up to receive free electronic health record and practice management software from San Francisco-based start-up Practice Fusion. Enterprise software for medical practices can cost $50,000. How can one company give away its e-record system at no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


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

weak security → breaches

- easy to hack
- weak authentication
- weak ‘role-based’ authorization → ‘insider’ snooping and theft
- data at rest, in use, in transit not encrypted
- P2P software leaks data
- web apps (SaaS/SSL) leak data*
- ease of copying, stealing, losing mobile devices
- de-identification and anonymization don’t work
- unsafe clouds

* http://www.informatics.indiana.edu/xw7/WebAppSideChannel-final.pdf


KING OF POP
MICHAEL
JACKSON
THIS IS IT

?????

?

?

??

?

Cost of Security Breaches

EXAMPLE: In 2006, Providence Health & Services paid a $95,000 penalty and provided two years of free credit monitoring to thousands of people after a car prowler broke into the van of a Providence employee who had left computer disks and data tapes inside. The records, some going back 20 years, contained Social Security numbers and medical information for 365,000 people. Providence spent $8-9M defending against a class action lawsuit.

- **Average direct, indirect, and opportunity costs to companies that experienced a data breach was $14 million/company.**
- average cost: $140/customer with breached data
- 100,000 is the average number of customers affected by security breaches

Laptop Data Breaches: Mitigating Risks Through Encryption and Liability Insurance

By Julie Machal-Fulks and Robert J. Scott,

http://www.scottandscottllp.com/main/uploadedFiles/resources/Articles/ArticleLaptop_Data_Breaches.pdf

Americans expect privacy and security,

but....

REALITY:

rampant data theft and a massive data mining industry thrives, while doctors and patients can’t access PHI

liability/reputation

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”

ideal HIT systems

THE TEXAS TRIBUNE

DNA Destruction

Emily Ramshaw
March 9, 2010 |

In the weeks before state health officials destroyed more than 5 million newborn blood samples they had stored without consent, privacy advocates, parents and lawmakers reached a last-ditch accord to save them — but couldn't convince the Department of State Health Services to sign on.

http://www.texastribune.org/stories/2010/mar/09/blood-drive/

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

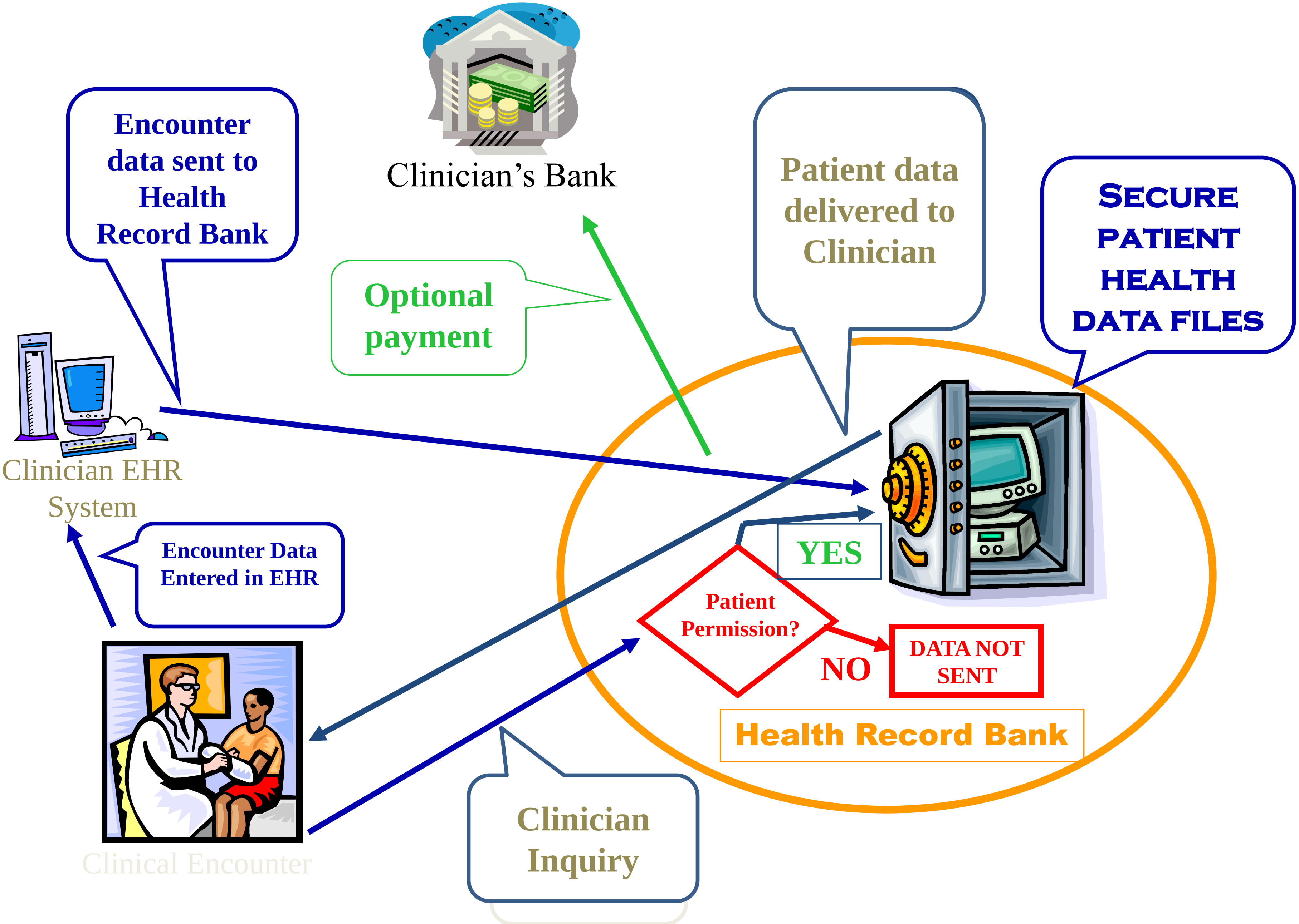
      (employees have unique access codes and can see selected data)


Your solution for controlling who sees your personal health information
Hello Cassandra Hoag (Sign Out)
PrivacyLayer™
Home
About PrivacyLayer
How it Works
Related Services
Support
Settings
My Health Universe
Privacy Concerns
New Opportunities
View within: Past 3 years
Devices
Blood Glucose Monitor
Heart Rate Monitor
Employers
Pharmacies
Rite Aid
Clinical Trials
Payers
Blue Shield of Ca
Aetna
Family & Friends
C. Hoag
W. Hoag
Hospitals & Care Centers
Hoag Hospital
Cedars Sinai Hospital
Mammoth Hospital
Newport Radiology
Pathology Partners
Hoag Cancer Center
Practitoners
Levine, MD
Shapiro, MD
Fong, MD
Park, MD
Control Panel
◂ Hide
Rotate Clockwise (Shift + Plus)
Rotate Counderclockwise (Shift + Minus)
Zoom In (Cntrl + Plus)
Zoom In (Cntrl + Minus)
Legend
◂ Hide
Allow All
Allow None
Allow Selected
Req. Attention
Pref. Not Set
(e.g., Defaults to applicable Federal or state law)
Introduction | Press | Partners | Careers | FAQs | Licensing Information | Privacy | Legal | Sitemap
© 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
   - ‘safe’ research without 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)

Health Record Bank



Clinician's Bank

Encounter data sent to Health Record Bank

Optional payment

Patient data delivered to Clinician

Secure patient health data files

Clinician EHR System

Encounter Data Entered in EHR

YES

Patient Permission?

NO

DATA NOT SENT

Health Record Bank

Clinical Encounter

Clinician Inquiry

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 patient file cabinet. In this situation, all patient information goes to a common location for the patient, and the patient can make decisions about sharing at that storage location

Anyone today who thinks the privacy issue has peaked is greatly mistaken*…we are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope.*

Forrester Research

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-4-2210.pdf
See NHIN slides at:
http://patientprivacyrights.org/wpcontent/uploads/2010/06/SweeneyTrustworthyNHINDesigns.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.*
http://patientprivacyrights.org/wpcontent/uploads/2010/02/Rothstein-ReIOM-Report.pdf

P2P leaks “Data Hemorrhages in the Health-Care Sector”, in *Financial Cryptography and Data Security, February 22-25, 2009 by M. Eric Johnson*
http://patientprivacyrights.org/media/JohnsonHemorrhagesFC09d.pdf