

Texas Public Health Committee

Patient Expectations for HIT:
Control over Health Records
Privacy Solutions for HIE

May 11, 2010

Deborah C. Peel, MD

patientprivacyrights

Patient expectations

Americans expect
control over personal
health data, 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. (*BEFORE the amended HIPAA Privacy Rule*)

HIPAA 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.

*"... 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 HHS HIPAA "Privacy Rule" which recognized the "right of consent".

*"....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".

*"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."*

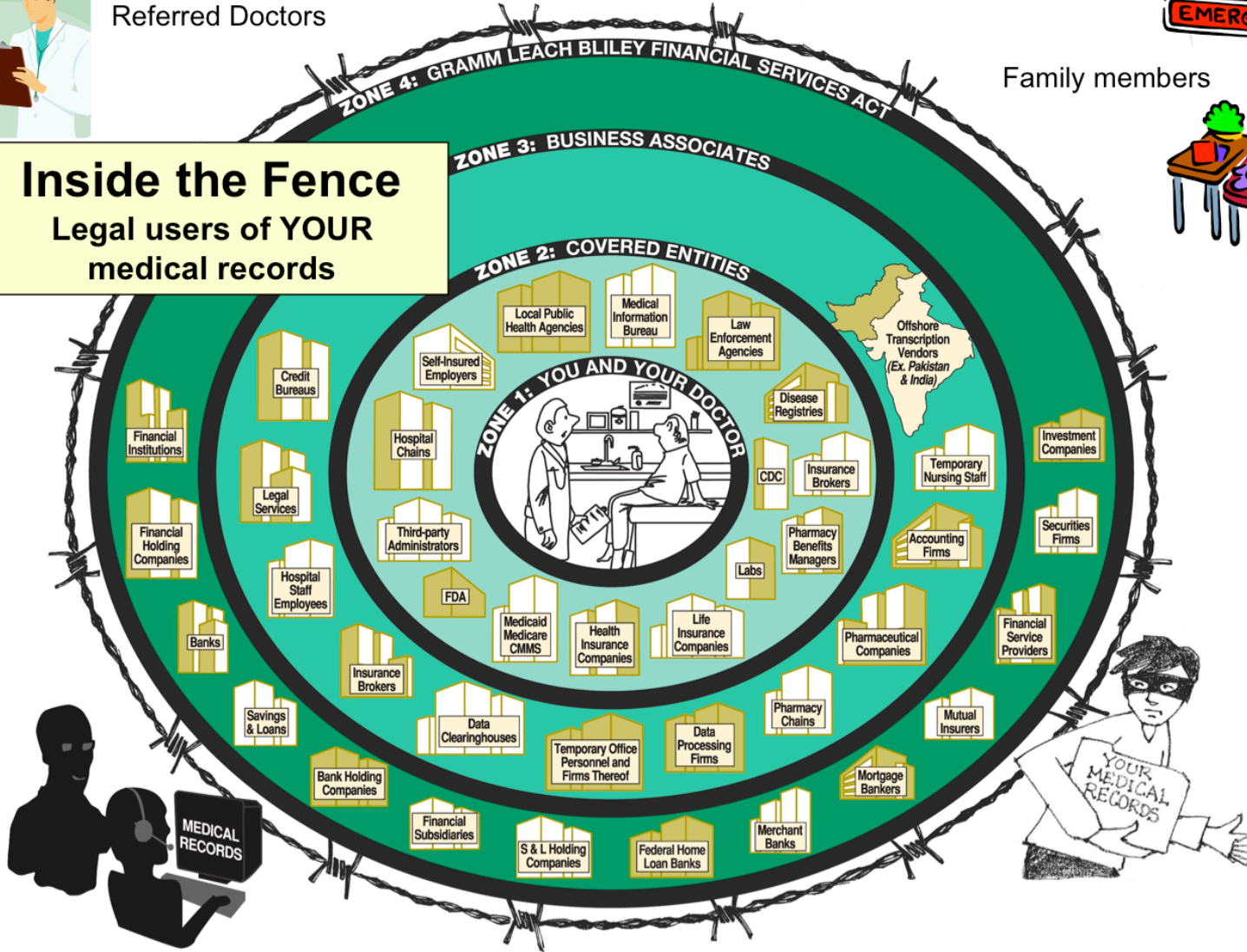


Referred Doctors



Family members

Inside the Fence
Legal users of YOUR medical records



Reality:
health data mining
industry

HIT

No privacy, weak security, data for sale

No privacy

- Over 4 million providers can access protected health information (PHI) for treatment, payment, and healthcare operations (TPO)
- No privacy, ie consumers do not control access to PHI

Weak security

- Easy to hack
- Even with role-based access, result is insider snooping and theft
- Strong 2nd factor authentication not required
- Encryption at rest, in use , and in transit not implemented
- Ease of copying, stealing, losing mobile devices

Secondary uses

The business model is selling data for secondary uses

**No trusted seals-of-approval for privacy (yet) and security (yet)
Industry seal-of-approval for security (HITRUST)**

Personal health data is for sale

Citation:

http://patientprivacyrights.org/media/Evidence_of_Disclosure.pdf

2010: Top Fortune 500 Companies in 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/



Clinical Data Services

<https://www.gehealthcare.com/portal/site/usen/menuitem.b399d8492e44a6765c09cbd58c829330/?vgnnextoid=ae0f4fb9eff5210VgnVCM100000382b3903RCRD&fromChannel=7e0f4fb9eff5210VgnVCM100000382b3903>

About 15,000 MDs (primary care, specialty)

De-identified, standardized data

Warehoused nightly

15 million unique patients, growing at 30% a year

The **de-identified data is collected from members using GE Centricity® Electronic Medical Record**. The database is used by outcomes researchers, members of the pharmaceutical industry, and academic institutions in the hopes of improving clinical care and outcomes throughout the healthcare industry.

The CDS Advantage Patient encounters since 1996; average 3 years data

Expanded demographic information (+ 3 digit zip code), insurance

Pharmaceutical therapeutic class, and brand name

Clinical Data Services

GE Healthcare's Clinical Data Services Business provides **access to de-**

identified ambulatory electronic medical record data. It is one of the

largest anonymized clinical databases in the

United States providing

access to real-world

longitudinal patient

information.



Clinical Data Services

The CDS Advantage

Disease Counts in Database

Hypertension 2,284,249
Hyperlipidemia 2,212,629
Depression 1,185,828
Cardiovascular Disease 1,004,214
GERD 984,864
Diabetes 922,169
Asthma 750,963
Osteoarthritis 602,043
COPD 319,310
ADD/ADHD/HKD 188,424
Rheumatoid Arthritis 85,757
Alzheimer's 35,790
Parkinson's 22,017

Note: Data reported as of
February 28th, 2010

Codified Medical Problems
Prescriptions/Historical Meds
Patient Allergies, Medical
Orders and Events
Vital Signs and Physical
Findings
Lab Values

[https://www2.gehealthcare.com/portal/site/usen/
menuitem.b399d8492e44a6765c09cbd58c829330/?
vgnnextoid=ae0f4fb9eff5210VgnVCM100000382b3903RCRD&fromChannel=7e0f4fb9eff
5210VgnVCM100000382b3903](https://www2.gehealthcare.com/portal/site/usen/menuitem.b399d8492e44a6765c09cbd58c829330/?vgnnextoid=ae0f4fb9eff5210VgnVCM100000382b3903RCRD&fromChannel=7e0f4fb9eff5210VgnVCM100000382b3903)

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 (?? hospitals sell data)
3	Express Scripts	#96	25 (sells Rx data)
4	Quest Diagnostics	#303	7 (sells data/sends data to HIEs)
<p>“transforms millions of test results into valuable information products” http://www.questdiagnostics.com/brand/careers/index.html#services</p>			
5	Omnicare	#347	6.3 (???)
<p>(leading Rx provider for seniors)“we capture a tremendous amount of data” ...combines data with outcomes algorithm technology</p>			
6	Lab Corp. of America	#442	4.7 (sells data??/sends data to HIEs)



What is BHI® (Blue Health Intelligence)?

share critical health information with employers

premier health intelligence resource in the nation

unmatched detail about healthcare trends and best practices while protecting individual privacy

BHI sets the new standard for healthcare data aggregation, reporting and analysis

Size and Value

- 1) **longitudinal data on 54 million BCBS members** [used for this purpose without consent]
- 2) 36 months of historical information
- 3) reporting not only by MSA, industry and product type, **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] throughout the collection and processing of **company data** [your health information is BCBS' corporate asset]
- 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>

Health Research Data for the Real World: the MarketScan Data Bases

David M. Adamson, PhD

Stella Chang, MPH

Leigh G. Hanson, MS, MBA

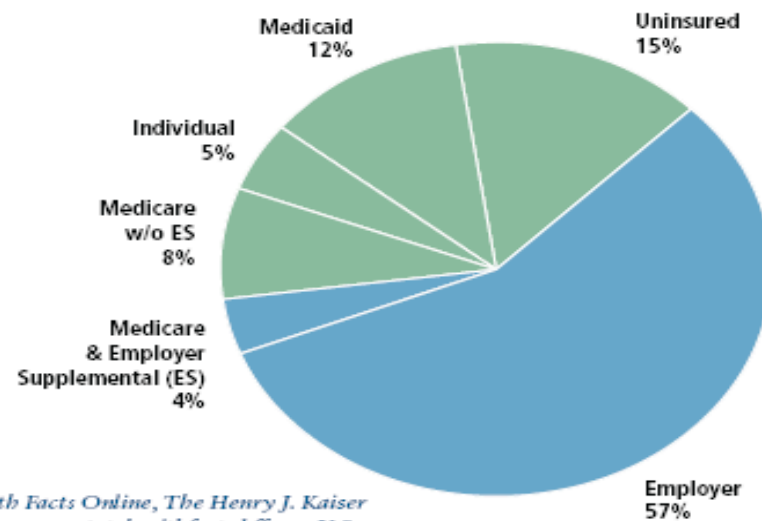
Research and Pharmaceutical Division

Thomson Medstat

January 2006

Medicare and Medicaid data is for sale

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.

Personal health information is for sale

Table 1: Sample Data Elements for Commercial and Medicare Databases

Demographic	Medical Information (Inpatient and Outpatient)	Health Plan Features	Financial Information	Drug Information	Enrollment Information
Patient ID	Admission date and type	Coordination of benefits amount	Total payments	Generic product ID	Date of enrollment
Age	Principal diagnosis code	Deductible amount	Net payments	Average wholesale price	Member days
Gender	Discharge status	Copayment amount	Payments to physician	Prescription drug payment	Date of disenrollment
Employment status and classification (hourly, etc.)	Major diagnostic category	Plan type	Payment to hospital	Therapeutic class	
Relationship of patient to beneficiary	Principal procedure code		Payments—total admission	Days supplied	
Geographic location (state, ZIP Code)	Secondary diagnosis codes (up to 14)			National drug code	
Industry	Secondary procedure codes (up to 14)			Refill number	
	DRG			Therapeutic group	
	Length of stay				
	Place of service				
	Provider ID				
	Quantity of services				

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	INTELLISCRIP
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

A man in a gym setting, wearing a headset and a sign that reads "VIAGRA FOR ERECTILE DYSFUNCTION". The background shows a woman on a treadmill.

TAKE **YOUR**
HEALTH DATA
"OFF THE MARKET".

watch the video ▶

CAMPAIGN for
PRESCRIPTION
PRIVACY

EMR vendor to share patient data with genetics research firm

3/20/2008 by Richard Pizzi

- “Perlegen Sciences, Inc., a company exploring the clinical application of genetic research, plans to collaborate with an undisclosed electronic medical records vendor to identify and develop genetic markers that predict how patients are likely to respond to specific medical treatments.
- Under the terms of the agreement, Perlegen, based in Mountain View, Calif. , will have exclusive access to the EMR vendor's database of U.S. records for the purpose of assessing and selecting patients from whom appropriate genetic samples could be collected.”

Practice Fusion expands, shows signs of rapid growth

By [Diana Manos, Senior Editor](#)

12/31/07

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.”***

Can we trust that
de-identified or
anonymized personal
information is truly
safe?

HIPAA allows use of “de-identified” data without consent

"I had learned that if I had the date of birth, gender and a five-digit zip code of a person, **I could identify 87 percent** of the people in the United States. So even if you don't give me your social security number, I can find out who you are nearly nine out of 10 times."

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

From *Scientific American* “Privacy Isn't Dead, or At Least It Shouldn't Be: A Q&A with Latanya Sweeney” <http://www.sciam.com/article.cfm?id=privacy-isnt-dead&page=3>

Prof. Latanya Sweeney on re-identification

*“Many details about our lives are documented on computers and when this information is linked together, the resulting profiles can be **as identifying as fingerprints** even when the information contains no explicit identifiers such as name and address...”*

*The time is right to seriously examine data collection and sharing practices...**The time to make policy changes is now in order to prevent data holders and governments from succumbing to the financial incentives that encourage sales of data.**”*

Prof. Latanya Sweeney

In *Southern Illinoisan v. Illinois Dept. of Public Health*, Dr. Sweeney testified that it was “very easy for anyone to identify persons from the [Illinois Department of Public Health’s] Cancer Registry using public data sets...all I used was commonly available PC technology, readily available software ...simple [spreadsheets].” [218 Ill.2d 390, 844 N.E. 2d 1, 300 Ill. Dec.329]

In 2005 Dr. Sweeney testified before the Department of Homeland Security noting that in 1997 she was able to find the medical record of Former Gov. William Weld (MA) by using just his date of birth, gender and zip code.

Testimony of Latayna Sweeney, PhD before the Privacy and Integrity

Advisory Committee of DHS, “Privacy Technologies for Homeland Security” – June 15, 2006

With just a few bits of information, Prof. Sweeney can re-identify **9 out of 10** people.

Scientific American “Privacy Isn't Dead, or At Least It Shouldn't Be: A Q&A with

Latanya Sweeney” <http://www.sciam.com/article.cfm?id=privacy-isnt-dead&page=3>

Weak Security

- Easy to hack
- Strong 2-factor authentication not required
- Data encryption at rest not required
- Loss/theft of mobile devices
- No role-based access, i.e., no consumer access controls (hacking from the inside)
 - Example: in an 8-hospital system all 33,000 employees can access every patient record

By [Pamela Lewis Dolan](#), amednews staff. *Posted May 4, 2010.*

Most health care information leaks have involved electronic systems, but some were paper-based. (new ARRA privacy protection)

HHS "started listing the breaches on its website in February, then updated the list in April."

"the reported incidents **affected 1,243,815 individuals.**"

Data indicate that "of the **64 breaches**...7 involved laptops, 12 involved paper records, 11 involved desktop computers, 8 involved either hard drives or network services, and 7 involved portable electronic devices."



2009 Data Breaches – Paper vs. Electronic Summary

Totals for Electronic records:

of Breaches: 369

of Records: 222,286,837

of Health records: 11,279,390

% of Breaches: 74.1

% of Records: 99.9

Totals for Paper records:

of Breaches: 129

of Records: 190,206

% of Breaches: 25.9

% of Records: .01

BUT in more than 52% of the breaches publicly reported, **NO statement of the number of records exposed is given.** Therefore, it is *unknown* how many total records may have been exposed due to breaches in 2009.



2009 - type of breach

2,532,674+	Data on the Move
21,780+	Subcontractors
8,501,878+	Hacking
3,317+	Accidental Exposure
13,871+	Insider Theft
245,698+	Unknown Attributes (type not reported)

Identity Theft Resource Center

<http://www.idtheftcenter.org/index.html>

Electronic medical records at risk of being hacked, report warns

CIO news

By Linda Tucci, Senior News Writer
19 Sep 2007 | SearchCIO.com

The electronic health record systems that automate the digitized medical histories of U.S. patients are severely at risk of being hacked, a new report has claimed.

"There was not one system we could not penetrate and gain control of data," said eHVRP board member Daniel S. Nutkis. "These systems were not any worse than banking systems. But the banking systems have elaborate security mechanisms sitting on top of them."

The eHVRP report is based on a **15-month study of more than 850 provider organizations.**

NIH Data Breaches

- **Barton health records stolen and he's ticked**
Dallas Morning News, April 3, 2008, by **Todd J. Gillman**
Rep. Joe Barton revealed Thursday that he is one [of the 3,000+] heart patients whose medical records were on an **unencrypted laptop** stolen from a National Institutes of Health researcher.
- ***New York Times* Editorial re: NIH Breach**, March 26, 2008
“There should be a federal law imposing strict privacy safeguards on all government and private entities handling medical data. Congress should pass a bill like the Trust Act, introduced by Representative Edward Markey, a Democrat of Massachusetts, imposing mandatory encryption requirements and deadlines for notifying patients when their privacy is breached. As the N.I.H. has shown, **medical privacy is too important to be left up to the medical profession.**”

Georgia Patients' Records Exposed on Web for Weeks

The New York Times, April 11, 2008, by Brenda Goodman

- A company hired by the State of Georgia to administer health benefits for low-income patients is sending letters to notify **tens of thousands of residents** that their **private records were exposed on the Internet for nearly seven weeks** before the error was caught and corrected, a company spokeswoman said on Thursday.
- **The records of as many as 71,000 adults and children enrolled in the Medicaid or PeachCare for Kids programs were inadvertently posted on Feb. 12**, said Amy Knapp, a spokeswoman for the company, WellCare Health Plans Inc., whose headquarters are in Tampa, Fla.

COMPUTERWORLD

Portable Storage Devices Pose IT Security Risk

How much damage can a memory stick or iPod do?
Plenty, say users and Analysts

March 27, 2006 ([Computerworld](#)) -- Baptist Memorial Health Care Corp. in Memphis, TN

- *users found it difficult to copy significant amounts of data to floppy disks, and the company "did not allow CD writers"*
- *users turned to "the USB flash drive, with enormous capacity and zero installation"*
- *only about 10% of companies have any policies dealing with removable storage devices*

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=management&articleId=109911&taxonomyId=14&intsrc=kc_feat

Los Angeles Times



Fawcett's cancer file breached

The incident occurred months before UCLA hospital employees were caught snooping in Britney Spears' files.

By Charles Ornstein April 3, 2008

No privacy

- Over 4 million ‘covered entities’, including providers, self-insured employers, data warehouses, etc, can access protected health information for treatment, payment, and healthcare operations
- Millions more ‘business associates’ can use data without consent
- Audit trails NOT required for all uses and disclosures

HHS citations: harms from lack
of privacy

Harms from lack of Privacy

- HHS estimated that **586,000** Americans did not seek earlier cancer treatment due to privacy concerns.
- HHS estimated that **2,000,000** Americans did not seek treatment for mental illness due to privacy concerns.
- **Millions** of young Americans suffering from sexually transmitted diseases do not seek treatment due to privacy concerns.

65 Fed. Reg. at 82,777

Harms from lack of Privacy

The California Health Care Foundation found that **1 in 8** Americans have put their health at risk *because of privacy concerns*:

- Avoid seeing their regular doctor
- Ask doctor to alter diagnosis
- Pay for a test out-of-pocket
- Avoid tests

Harms from lack of Privacy

- The Rand Corporation found that 150,000 soldiers suffering from PTSD do not seek treatment because of privacy concerns
- The lack of privacy contributes to the highest rate of suicide among active duty soldiers in 30 years

“Invisible Wounds of War”, the RAND Corp., p. 436, (2008)

NIH: harms from lack of
privacy

Insurance Fears Lead Many to Shun DNA Tests

By [AMY HARMON](#)

Published: February 24, 2008



Katherine Anderson, seen in a checkup last week, developed a blood clot last year partly due to an undiagnosed genetic condition.

“It’s pretty clear that the public is afraid of taking advantage of genetic testing,” said Dr. Francis S. Collins, director of the National Human Genome Research Institute at the [National Institutes of Health](#).

“If that continues, the future of medicine that we would all like to see happen stands the chance of being dead on arrival.”

Americans expect
control over
personal health
data, but.....

What does 'privacy' mean?

- The *Hippocratic Oath* says “Whatsoever I shall see or hear of the lives of men or women which is not fitting to be spoken, I will keep inviolably secret.”

What does 'privacy' mean?

- The *Code of Fair Information Practices (1974)* says “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.”

What does 'privacy' mean?

- The *NCVHS* (June 2006, Report to Sec. Leavitt) defined health information privacy as “an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data”. (Definition originally from the IOM)

AHRQ: 2009

20 focus groups

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.** This belief was expressed not necessarily because they want to prevent some specific use of data but as a **matter of principle.** (AHRQ p. 18)
- Participants overwhelmingly want to be able to **communicate directly with their providers with respect to how their PHI is handled, including with whom it may be shared and for what purposes.** Most believe they should automatically be granted the right to correct misinformation. (AHRQ p.33)

“there was **no support for the establishment of general rules that apply to all health care consumers.**

Participants thought that health care *consumers should be able to 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

NPR/Kaiser/Harvard 2009 Poll

The Public and the Health Care Delivery System

59% are NOT confident that if their medical records and PHI were stored electronically and shared online, that those records would remain confidential

NPR/Kaiser/Harvard 2009 Poll

76% believe it likely that an unauthorized person would get access to their medical records if the US adopts a system where medical records are kept electronically and shared online.

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

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.

Research on Consent and NBS Programs

From Public Health Genomics

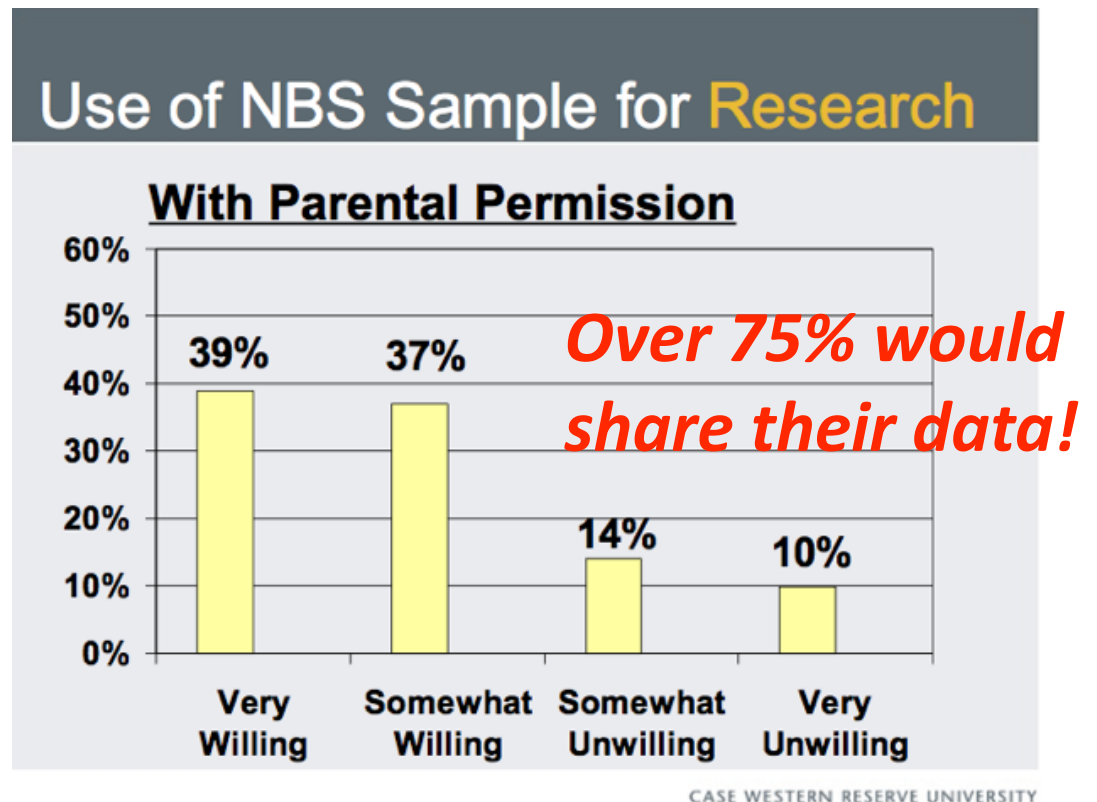
When Asked, Consumers Support Use of Their Data

*"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*

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



If
When Asked, Consumers Support Use of Their Data

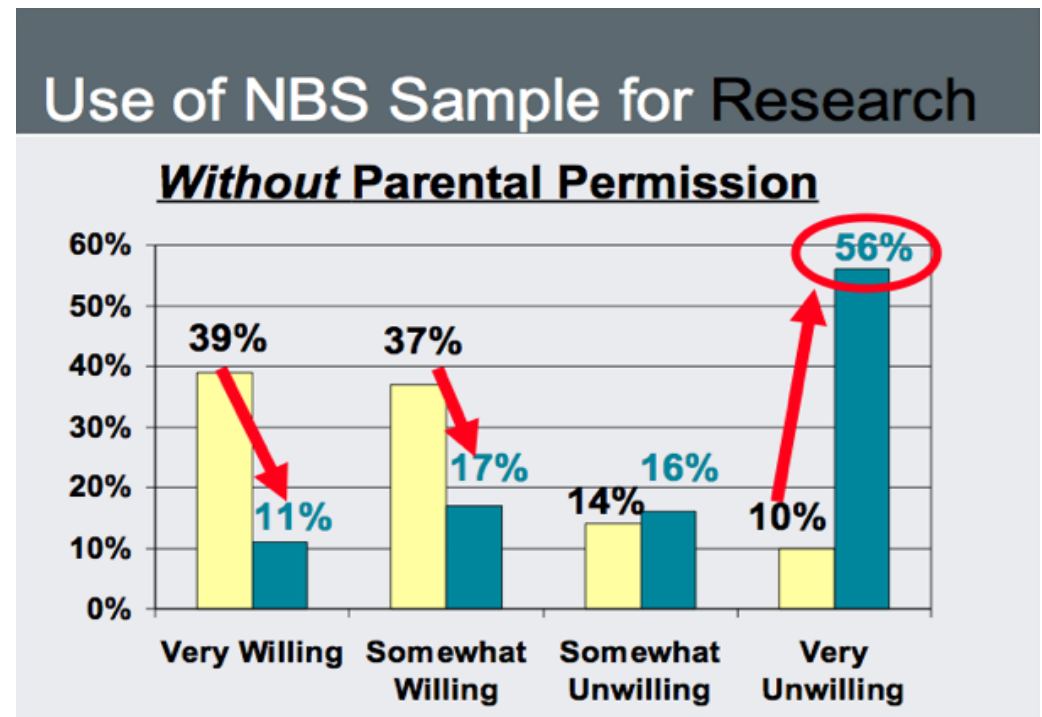
*"How willing are you to have your child's blood sample (from newborn screening) used for future research studies, with (or **without**) your permission?"*

WITHOUT CONSENT Only 28% were OK with research and 72% were NOT OK with research use

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).



Patients rights

10 Million Americans Expect Privacy

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.

Constitutional rights to privacy

"The right to be let alone is the most comprehensive of rights and the right most valued by civilized men.

To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the [Constitution]."

Olmstead v. United States, 277 U.S. 438, 478, 48 S.Ct. 564, 572
(1928) (Brandeis dissent)

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).

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 rights
legal privileges
common law

The ethical codes of all health professions require informed consent

Since the time of Hippocrates physicians have pledged to maintain the secrecy of information they learn about their patients, disclosing information only with the authorization of the patient or when necessary to protect an overriding public interest, such as public health. ***Comparable provisions are now contained in the codes of ethics of virtually all health professionals.***

Report to HHS, NCVHS (June 22, 2006)

Research ethics protect privacy

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

A. INTRODUCTION

5. In medical research on human subjects, considerations related to **the well-being of the human subject should take precedence over the needs and interests of society.**

B. BASIC PRINCIPLES FOR ALL MEDICAL RESEARCH

10. **It is the duty of the physician** in medical research **to protect the** life, health, **privacy**, and dignity of the human subject.

21. The right of research subjects to safeguard their integrity must always be respected. **Every precaution should be taken to respect the privacy of the subject**, the confidentiality of the patients information, and to minimize the impact of the study on the subject's physical and mental integrity and on the personality of the subject.

Key State Privacy Rights

- 10 state constitutions have the right to privacy
- Other state laws require extra privacy/consent protections for the disclosure of genetic tests, mental health records, sexually-transmitted diseases, and sensitive information related to reproduction and minors (check specifics)
- Consent is required by the AMA Code of Medical Ethics
- Consent may be required by physician licensing laws, by state law, and/or as the standard of practice in the community

Reality
today

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
- Segmentation---delayed
- Audit trails x 3 years---2011 or later
- Breach notice---2010
- Encryption
- Patient can prevent disclosures of PHI for 'payment and healthcare operations' if pays out-of-pocket--not addressed
- Consent Technologies---2014 or later

Consequences

No right to privacy & no federal definition of 'privacy'

- > 4 million Covered Entities (CEs) have access to PHI for TPO
- Millions of employees of CEs and Business Associates (BAs) access PHI
- No privacy, ie consumers do not control access to PHI

Weak security

- Easy to hack (security far weaker than commercial & financial industry standards)
- Role-based access, i.e., (allows massive 'insider' snooping and theft)
- Strong 2nd factor authentication for access not required
- Encryption at rest, in use, in transit not implemented
- Ease of copying, stealing, losing mobile devices

Secondary use of data

The business model for many HIT systems is selling data

**No trusted seals-of-approval for privacy (yet) and security (yet)
Industry seal-of-approval for security (HITRUST)**

EHRs without consent
PHRs without consent
HIEs without consent
NHIN without consent
Research without consent

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>

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*.

Liability

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”

Sweeney's Congressional briefing on defects of MU and NHIN/HIEs

- **Secondary use of protected health information (PHI) by Business Associates is “unbounded, widespread, hidden, and difficult to trace.”**
- Implementing EHRs that meet 'Meaningful Use' criteria will “increase data sharing, but adding the NHIN will massively increase data sharing.”
- There are **significant defects in the two National Health Information Network models** which are supposed to link all Americans' health information online that HHS plans to implement.
- The proposed NHIN models aren't capable of exchanging enough needed health data (i.e., do not have enough "utility") nor do they permit patients to have any control access sensitive health data by the millions of "Covered entities" and their employees who will use the NHIN (i.e., do not offer enough "privacy").

In other words, the NHIN solutions currently on the table give Americans the worst of both worlds: no privacy (ie no patient control over personal health information) and the inability to exchange all the health information needed for clinical and other uses.

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

Patient-centered

Solutions:

consent tools

health banks

HIEs/NHIN

Solutions:

Meet demand for privacy
via
privacy-enhancing
technologies

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/>

Guaranteed Health Data Privacy

1. Adapt/use the National Data Infrastructure Improvement Consortium (NDIIC) open source electronic consent module as the minimum standard for consent tools in PHRs and for all HIT
2. Require the strong privacy protections in 42 CFR Part 2 be extended to cover all personal health information (PHI), wherever it is held.

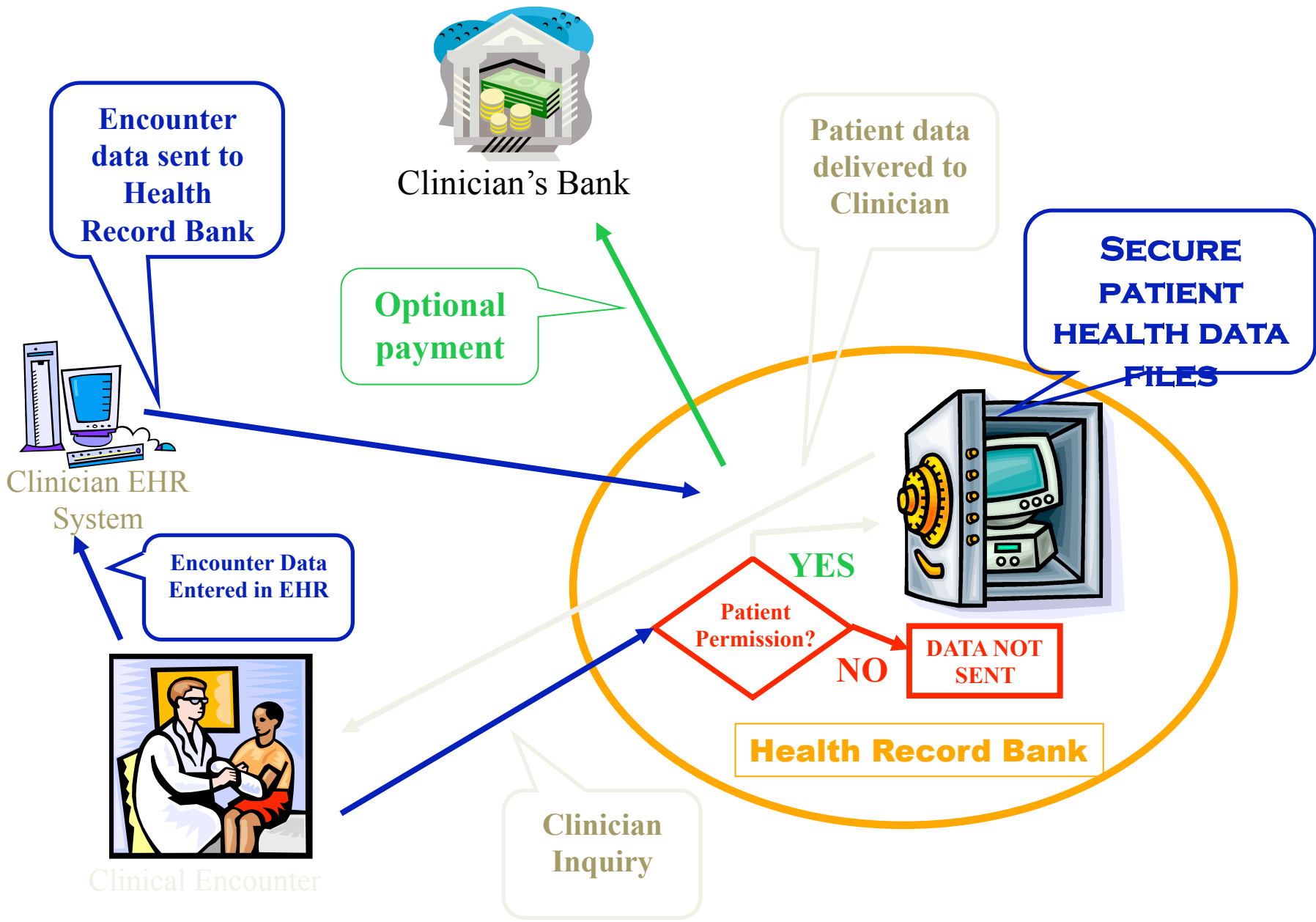
<http://www.ndiic.org/>

Guaranteed Data Privacy

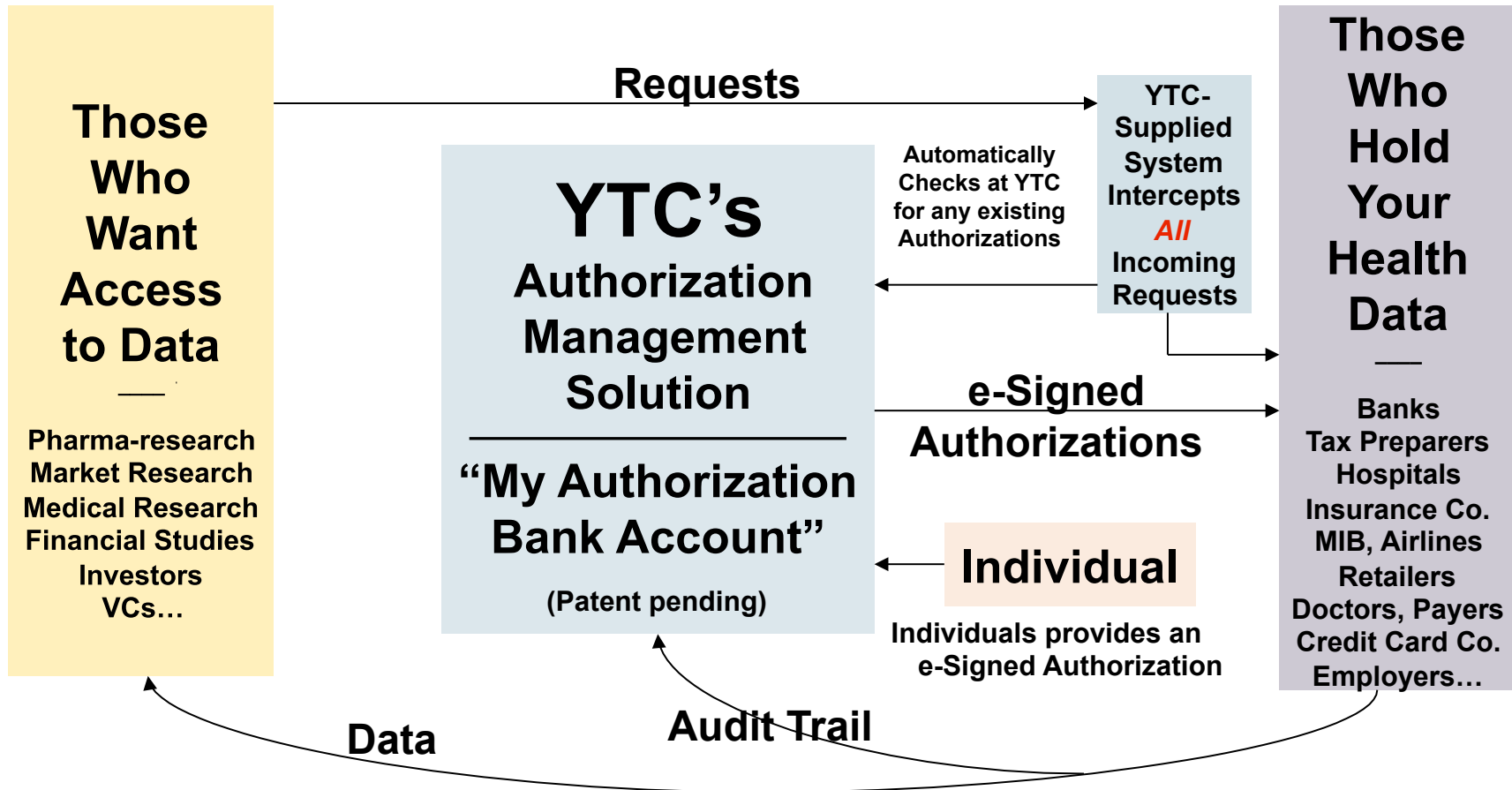
1. Adapt/use the National Data Infrastructure Improvement Consortium (NDIIC) open source electronic consent module as the minimum standard for consent tools in PHRs and for all HIT
2. Require the strong privacy protections in 43 CFR Part 2 be extended to cover all personal health information (PHI), wherever it is held.

<http://www.ndiic.org/>

Health Record Bank



Example: independent consent tool



NOTE: YTC never sees, nor stores your data

Consent Solutions So Far for Research Biobanks

Each person grants “private access” to all or selected parts of their personal information based on their particular needs and interests



Your solution for controlling who sees your personal health information

PrivacyLayer

Home About PrivacyLayer How It Works Related Services Support Contact Us

“ You can trust PrivacyLayer to let you manage who can and cannot gain access to your health information. ”

LeRoy E. Jones*, CISSP
Chief Executive of GSI Health, Inc.
Program Manager, Healthcare IT Standards Panel
*Chief Technology Officer for Private Access LLC

PRIVACY ASSURED with PrivacyLayer™

Toolbox

- My Account
- My Family
- Privacy Settings
- Privacy Alerts
- Audit Log
- Toolbox Help

Your Privacy is Our Priority Manage Your Records



PrivacyLayer™ makes it easy to select your privacy preferences. Click on the green, yellow or red buttons to select your preferences. When you decide which description and settings best describe your preferences, click the “Next” button found below.

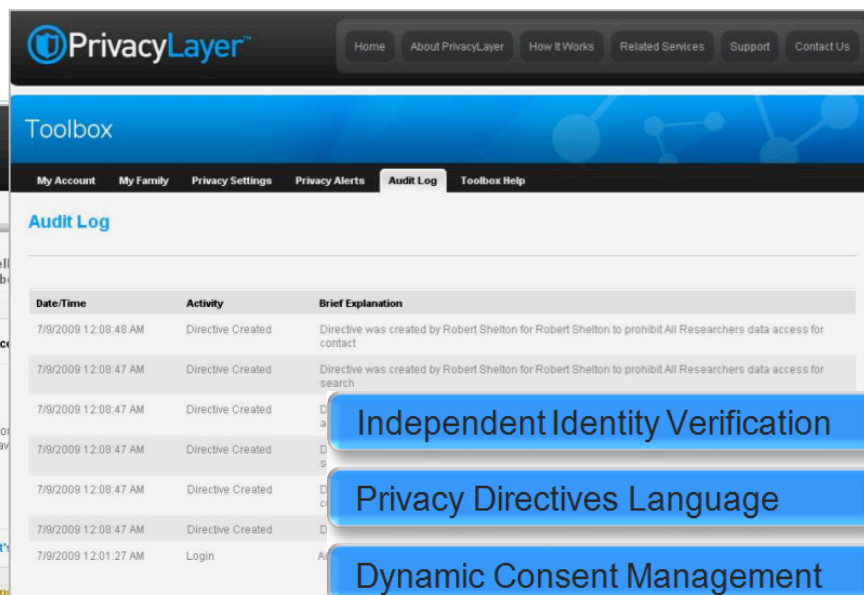
Lower privacy concerns Moderate privacy concerns Greater privacy concerns

Here's what your guide suggests if you have greater privacy concerns:

“ I realize that some value privacy to the point where they're uncomfortable disclosing their condition (condition) to someone they don't know. In that case, I'd suggest these settings, where you'll always have to learn more before you provide any contact details. ”

Researcher & Research Groups	Search Preferences what's this?	Contact Preferences what's this?
Dr Giedd	Allow to see my anonymous information	Notify me so I can consent
All KS&A Researchers	Allow to see my anonymous information	Notify me so I can consent or decline contact
All Researchers	Prohibit from searching	Prohibit all contact

Choose a different guide Customize Next



PrivacyLayer

Home About PrivacyLayer How It Works Related Services Support Contact Us

Toolbox

My Account My Family Privacy Settings Privacy Alerts Audit Log Toolbox Help

Audit Log

Date/Time	Activity	Brief Explanation
7/9/2009 12:08:48 AM	Directive Created	Directive was created by Robert Shelton for Robert Shelton to prohibit All Researchers data access for contact
7/9/2009 12:08:47 AM	Directive Created	Directive was created by Robert Shelton for Robert Shelton to prohibit All Researchers data access for search
7/9/2009 12:08:47 AM	Directive Created	Directive was created by Robert Shelton for Robert Shelton to prohibit All Researchers data access for search
7/9/2009 12:08:47 AM	Directive Created	Directive was created by Robert Shelton for Robert Shelton to prohibit All Researchers data access for search
7/9/2009 12:08:47 AM	Directive Created	Directive was created by Robert Shelton for Robert Shelton to prohibit All Researchers data access for search
7/9/2009 12:08:47 AM	Directive Created	Directive was created by Robert Shelton for Robert Shelton to prohibit All Researchers data access for search
7/9/2009 12:01:27 AM	Login	Account was accessed by Robert Shelton

- Independent Identity Verification
- Privacy Directives Language
- Dynamic Consent Management
- Comprehensive Audit Tracking
- Integrated eCommerce Features

ABRC Biospecimen Locator Service

... consent can be integrated into cutting-edge applications such as services for locating biospecimens for use in qualified research projects

Arizona Biospecimen Locator

Home Search Consortium Information

Find biospecimens to use in qualified research projects.

The Arizona Biospecimen Locator (ABL), a service of the Arizona Biomedical Research Commission, is a centralized, web-based biospecimen database of tissue stored at participating Arizona hospitals and tissue banks. Researchers may use this site to browse, search and request biospecimens to use in qualified studies.

Overview | How to use this site | Eligibility | FAQ | Register

Sign In

Email Address: pch-tech@example.com

Password: *****

Sign In

Forgot Password? | Register

Browse By Type

- Cells (0)
- Fluid

Browse By Disease

- Malakoplakia of stomach (disorder) (1)
- Infantile atopic dermatitis (disorder) (3)
- Benign neoplasm of parietal lobe (disorder) (2)

Welcome

Have you ever needed access to high quality biospecimens to use in research? The Arizona Biospecimen Locator can help.

Arizona Biospecimen Locator

Welcome, PCH Account Cart My Requests Help Sign Out

Home Search Consortium Information Administration

Biospecimen Administration

Add New Biospecimen

Filter By Status: All

Search By External ID: Search

Biospecimen ID	Type	Pathological Diagnosis	Anatomic Site	Available Quantity	External ID (Record ID)	Fee	Status	Action
64016	Tissue	Acute and chronic colitis (disorder)	Intestine - Large	100 mg	264016	\$50.00 - \$500.00	Shipped	Edit
64017	Plasma	Acute and chronic colitis (disorder)	Intestine - Large	200 ml	264017	\$50.00 - \$300.00	Available	Edit
64018	Serum	Acute and chronic colitis (disorder)	Intestine - Large	150 ml	264018	\$50.00 - \$300.00	Available	Edit
64019	Tissue	Acute pancreatitis (disorder)	Pancreas	100 mg	264019	\$50.00 - \$500.00	Available	Edit
64020	Plasma	Acute pancreatitis (disorder)	Pancreas	200 ml	264020	\$50.00 - \$300.00	Available	Edit
64021	Serum	Acute pancreatitis (disorder)	Pancreas	150 ml	264021	\$50.00 - \$300.00	Under Review	Edit
64022	Tissue	Adenocarcinoma of stomach (disorder)	Stomach	50 mg	364022	\$80.00 - \$400.00	Under Review	Edit
64023	Plasma	Adenocarcinoma of stomach (disorder)	Stomach	100 ml	364023	\$80.00 - \$200.00	Available	Edit
64024	Serum	Adenocarcinoma of stomach (disorder)	Stomach	100 ml	364024	\$80.00 - \$200.00	Under Review	Edit

Research Opportunity Requires Your Attention

Researcher: Jay Giedd KS&A
11 Keats Court
Coto de Caza, CA 92679
Phone: (888) 999-9428

Helpful Links:
[More about this researcher](#)
[More about this research](#)

Pending Actions:
⚠ The researcher noted above has requested contact information for **Chris Briggs**.
Purpose: Specific study or trial; ID: NCT00001246
Trial Name: Brain Imaging of Childhood Onset Psychiatric Disorders, Endocrine Disorders and Healthy Children
[View Details](#)

Explanation: According to your current privacy settings, you wish to be notified in advance when a researcher wants your contact information. This "Research Opportunity" is that notice. Be aware that the researcher noted above has agreed to the Terms of Use for your contact information. You can now give permission (or your "express consent") for the contact information to be shared with the researcher; you can evaluate the opportunity and decline to share the contact information, or you can consider this opportunity later by clicking the "snooze" button.

Your Alternatives: [what's this?](#) [Consent](#) [Decline](#) [Snooze](#)

Open Source Consent Solutions

1. Adapt/use the National Data Infrastructure Improvement Consortium (NDIIC) open source electronic consent module as the minimum standard for consent tools in PHRs and for all HIT
2. Require the strong privacy protections in 43 CFR Part 2 be extended to cover all personal health information (PHI), wherever it is held.

Audit trails based on authentication

Mar 01, 2010

PrivacyAlert™ Quickly Detects Snooping and Identity Theft of Medical Records

detects snooping, identity theft, and inappropriate access of medical records

automated and scalable privacy monitoring solutions

assist in investigating and reporting on patient data privacy breaches

ability to set and focus investigation criteria on employee, patient or combination of both

Out-of-the-box support for all leading healthcare applications including Eclipsys, GE Centricity Enterprise, MEDITECH Magic, Siemens Invision and others.

<http://www.marketwire.com/press-release/Imprivatas-New-Product-Helps-Hospitals-Proactively-Investigate-Audit-Access-Patient-1123908.htm>

Deborah C. Peel, MD

Founder and Chair

(O) 512-732-0033

dpeelmd@patientprivacyrights.org

www.patientprivacyrights.org

patientprivacyrights