

5<sup>th</sup> Annual Ohio Health IT Summit

**Keynote Address:  
Protecting Privacy While Expanding  
HIT and HIE**

Monday, October 27, 2008

Deborah C. Peel, MD

patientprivacyrights

# Self-regulation and Deregulation

Are there parallels between the  
financial and the healthcare  
systems?

## Greenspan: I Was Wrong to Trust Banks

“Those of us who have looked to the self-interest of lending institutions to protect shareholders' equity (myself especially) are in a state of shocked disbelief.”

Asked if he was wrong to champion deregulation, Greenspan replied, “partially,” explaining he’d believed lending institutions were the ones in the best position to protect their shareholders’ interests.

<http://www.newser.com/story/40718/greenspan-i-was-wrong-to-trust-banks.html>

Health IT:  
the self-regulation of  
security

## Electronic medical records at risk of being hacked, report warns

### CIO news

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

"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.

## The Wall Street Journal

### Are Your Medical Records at Risk?

Amid Spate of Security Lapses, Health-Care Industry Weighs Privacy Against Quality Care  
By SARAH RUBENSTEIN April 29, 2008; Page D1

## Breaches of consumers' confidential data are widespread in the health-care industry.

But hospitals are notable for the sheer number and types of employees – including billing staff, nurses, doctors, researchers and lab technicians -- who have quick access to individuals' private information.

[http://online.wsj.com/article/SB120941048217350433.html?mod=loomia&loomia\\_si=t0:a16:g2:r2:c0.156457](http://online.wsj.com/article/SB120941048217350433.html?mod=loomia&loomia_si=t0:a16:g2:r2:c0.156457)

## 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."



## 2008 Data Breach Stats – Paper vs. Electronic Summary

### Totals for Electronic records:

# of Breaches: 360

# of Records: 21,531,952

# of Health records: 7,033,064

% of Breaches: 80.2

% of Records: 97.5%

### Totals for Paper records:

# of Breaches: 89

# of Records: 559,386

% of Breaches: 19.8

% of Records: 2.5%

## 2008 total breaches of health records (to date)

4,349,087+ Data on the Move  
2,241,363+ Subcontractors  
12,000+ Hacking  
335,805+ Accidental Exposure  
94,809+ Insider Theft  
**7,033,064**

### Identity Theft Resource Center

[http://www.idtheftcenter.org/artman2/publish/lib\\_survey/ITRC\\_2008\\_Breach\\_List.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml)

## Health IT: the deregulation of privacy

## HHS 'deregulated' Americans' rights to health privacy in 2002

### 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)

## What does 'privacy' mean?

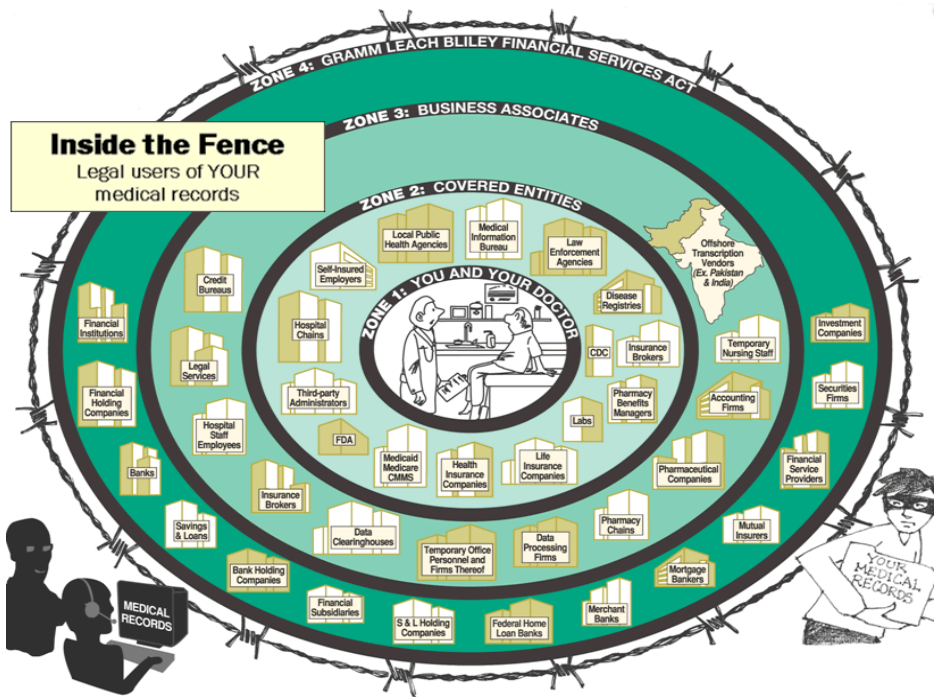
Legal definition: 'privacy' means control over personal information

No control = no privacy

HHS and Congress have not defined 'privacy'

## Elimination of Consent

1996	Congress passed HIPAA, <u>but did not</u> 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]... <b>detailed recommendations on standards with respect to the privacy of individually identifiable health information.</b> "
2001	President Bush implemented the HHS HIPAA "Privacy Rule" which recognized the "right of consent".	"...a covered health care provider <b>must obtain the individual's consent</b> , 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 <b>consent provisions...are replaced</b> with a new provision...that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations."

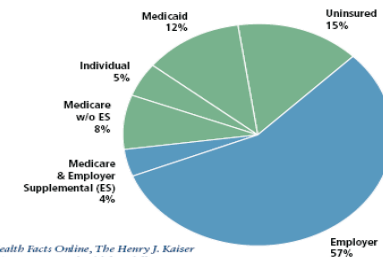


deregulation of HIPAA  
ensures  
the commoditization  
of personal health  
information

Personal health data  
is for sale

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](http://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				

## Healthcare IT News

### 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.”

## Healthcare IT News

### 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.”***

## Prescription Data is for sale

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](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	INTELLISCRIPPT
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

## Nex2, Inc. (Sold to United Healthcare in 2002)

- In stealth-mode, Nex2 built what are arguably the largest, near-realtime drug history databases in the world, with over 200 million Americans' five-year running drug histories online (over 12 TB total). The databases are updated every 24 hours by every retail pharmacy in America via the PBMs... [these] prescription profiles act as a powerful surrogate for the medical record itself.
- **All of this is HIPAA compliant because the insurance company always has the release, signed by the individual applicant.**
- United Healthcare's Ingenix unit now runs these massive virtual database operations, still in stealth-mode, for obvious reasons.

## Prescription data mining

The top three publicly-held prescription data mining and sales corporations in the US reported revenues in 2007 of \$65 billion dollars.

See Fortune 500's data on their revenues at:

<http://money.cnn.com/magazines/fortune/fortune500/2008/snapshots/10630.html>.



# Insurers sell data

In August, 2006, a large insurer, with plans in all 50 states, announced the creation of a new business unit to aggregate and sell the claims and health records of 79 million enrollees:

The Medical Director said that the intended use of the database is to “service the big employers that pay the bills and want to pay smaller bills for health insurance.”

He was “very enthralled about the ability to help multi-state employers fix their healthcare costs.” During the one and one-half years that the plan had been building the database, he had “never heard about privacy concerns.”

## EHRs and PHRs:

### 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
- No role-based access, i.e., (insider snooping and theft)
- No strong 2<sup>nd</sup> factor authentication
- No encryption at rest
- Ease of copying, stealing, losing mobile devices

#### Secondary uses

- The business model for many EHRs and PHRs is selling data for secondary use and data mining

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

The current  
Administration:  
expanding  
self-regulation  
and deregulation



## Current Administration

- HIT Strategic Plan: all EHRs and PHRs will be data mined for “population health”
- GAO: HHS has not ensured that privacy principles are addressed and may fail to establish the public’s trust
- NCVHS promotes "secondary uses" of PHI without contemporaneous, informed consent
- ONC Report on Data Quality recommends open access to all EHRs by health plans to detect fraud

## HHS/ONC Federal Health IT Strategic Plan: 2008-2012

June 3, 2008

### HIT Strategic Plan: privacy problems

- “Population health” use of data trumps American’s rights to health privacy
- All EHRs and PHRs are to be designed for data mining and use without consent for “population health”
- The American public has never debated the question of whether ALL electronic health records should be open for research and “population health” uses without informed consent

### Goal One – *Enable Patient-focused Health Care*

**Enable** the transformation to higher-quality, more cost-efficient, patient-focused health care through **electronic health information access and use by care providers, and by patients and their designees.**

## Goal Two – *Improve Population Health*

**Enable** the appropriate, authorized, and timely **access and use of electronic health information to benefit public health, biomedical research, quality improvement, and emergency preparedness.**

## Strategies for Objective 2.2

The following illustrative action steps seek to advance EHR interoperability to include standards, technical architecture and certification requirements that support data sharing and use for population health purposes:

Define and prioritize a set of consensus based data and technical standards for EHRs that are needed to enable population health uses through interoperable health information networks.

Page A17

## Strategies for Objective 2.2

**Strategy 2.2.2:** Allow for flexibility in the models for the exchange of health information (organizational, geographic, and personally controlled), while still advancing the specific standards and policies necessary to ensure that they all work together to meet population health needs.

Page A17

## GAO report Sept 2008

Health Information Technology:  
HHS Has Taken Important Steps  
to Address Privacy Principles and  
Challenges, Although More Work  
Remains

## GAO conclusions

Unless HHS's privacy approach includes a defined process for assessing and prioritizing the many privacy-related initiatives, the department may not be able to ensure that key privacy principles and challenges will be fully and adequately addressed.

Further, stakeholders may lack the overall policies and guidance needed to assist them in their efforts to ensure that privacy protection measures are consistently built into health IT programs and applications.

As a result, the department may miss an opportunity to establish the high degree of public confidence and trust needed to help ensure the success of a nationwide health information network.

## NCVHS Report 2007

Report to the Secretary of the U.S. Department of Health and Human Services

on

**Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data**

October 21, 2007

## NCVHS

The report recommends that HHS allow "secondary uses" of our PHI without contemporaneous, informed consent.

"Secondary uses" include research, marketing, monitoring, data mining and profiling.

- sale of PHI is allowed
- your right of consent is eliminated
- expands access to your data
- enables tracking of you and your doctors
- enables data mining, patient profiling and data linking

## Recommended Requirements for Enhancing Data Quality in Electronic Health Records

Final Report  
May 2007

**The Office of the National Coordinator for Health Information Technology**

Prepared by RTI International

## ONC/RTI Report May 2007

In 2003, losses due to fraud were \$51 billion to \$170 billion.

Moving to an electronic environment has the potential to greatly increase fraud.

The use of advanced analytics software built into the NHIN is critical to fraud loss reduction.

## Fraud is due to unauthorized access to EHRs

THE ONC SOLUTION: Build open access into EHRs so payers can detect fraudulent patterns. Payers (insurers, employers, and government) are granted full access to PHI to detect fraud.

THE PRIVACY SOLUTION: Consumers prevent fraud by limiting improper/unwanted access to their EHRs using electronic consent management tools.

## Key Quotes from ONC/RTI Report

Detection of a fraudulent claim is often difficult when a payer has access only to EHR information for a single encounter.

Reviewing information over an entire episode of care for a single patient allows greater ability to detect fraud.

## Will the next Administration restore privacy?

The next Congress  
and Administration  
are not likely to  
restore privacy.....

unless YOU act

### 3 Things You Can Do Now

- Sign up for e-Alerts
- Tell Congress: “Don’t pass health IT legislation without strong privacy protections”
- Use the Consumer Tool Kit, ask providers to sign your privacy forms

[www.patientprivacyrights.org](http://www.patientprivacyrights.org)

‘Smart’ consumers



patientprivacytoolkit  
hericuhb iasclrooikic

#### Forms

- [Privacy Instructions](#): Give to all Providers
- [How to Talk to Your Doctor](#)
- For Physicians: [Opt out of the AMA Database](#)

#### Information

- [Your Health Privacy Rights](#)
- [FAQs](#)

#### Take Action

- [Stay Informed](#)
- Sign the Campaign for Prescription Privacy [Petition](#)
- [Advocacy 101](#): How to Talk to the Folks You Vote For (or Against)

#### Forms

- [Complaint Form to HHS](#)
- Withdraw Consent -- *coming soon*

#### Information

- [FAQs](#)

#### Take Action

- [Congress Needs to Hear from You](#)
- [Share Your Story](#)

# Online Privacy Education

## patientprivacyrights

Personal Health Records Latest Battle in Assault on Medical Privacy

Patient Privacy Rights is advising members NOT to sign up for personal health records (PHRs). PHRs are simply the latest battlefield to invade medical privacy.

Despite the promise of great convenience, PHRs have no legal or ethical protections for the sensitive health information patients, insurers, or employers place in them. Today, insurers and employers are rapidly pressing the public to use PHRs in databanks that the public does NOT own or control. Wal-Mart, Intel, and other major employers formed Oposia to bank employees' PHRs. The major insurers are also setting up PHR databanks they will pre-populate with enrollees' health and claims data (and enrollees may not be able to opt-out of these data banks). Even banks and financial institutions are rushing to get into the business of holding your PHR along with your money. And the public trusts none of them.

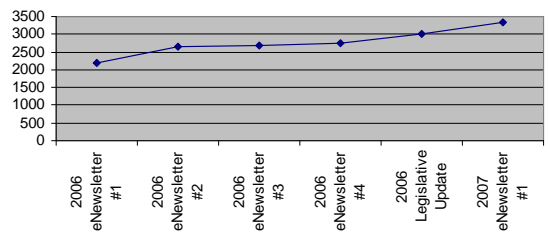
So, before signing up for a PHR, Patient Privacy Rights urges all citizens to read this January 5, 2007 review commissioned by the Office of the National Coordinator for Health IT (ONCHIT). It contains Patient Privacy Rights' cautionary statements against PHRs.

- See Patient Privacy Rights' summary of the ONCHIT report
- See SA ONCHIT report
- See Patient Privacy Rights' press release on PHRs



- Regular Newsletter keeps general public aware of medical privacy issues.
- Audience continues to grow

PPR eNewsletter Audience



# On-line resources for consumers



- Online Library
  - Comprehensive medical privacy library of news stories, reports and polls
- On-line resource for policy experts, media and legislative staff
- Ongoing email outreach program to keep consumers engaged

# Privacy e-campaigns

## SIGN THIS PETITION

- I want to decide who can see and use my medical records
- I do not want my medical records or those of my family's to be seen or used by my employer
- I should never be forced to give up my right to privacy in order to get medical treatment

Yes, I want my medical privacy! \*\*\* = Required Fields

Name:  First  Last

\* Email:

ZIP / Postal Code:

Yes, I want Privacy Rights

Remember



Tell Congress You Want to Control Who Can Access Your Medical Information

Do you want to control who can access and use your medical information? You won't, unless we act today!



Congress is currently considering legislation to create electronic health networks that would expose our medical records to a web of interests.

Electronic health networks can reduce costs, reduce errors and improve medical care. But without ironclad privacy protections these networks will open our most personal medical records to prying eyes. Employers, banks, marketers, insurers and pharmaceutical corporations can access and use your medical data for purposes that have

nothing to do with your medical care (read Consumers Union "The New Threat to Your Medical Privacy," for more information).

- "I Want My Medical Privacy" Petition recruited 3,000 individuals to medical privacy efforts

- Use e-campaigns to contact state and federal lawmakers

- Use online polls and surveys engage and educate the public.



# patientprivacyrights

Dear Abby:

Our next President faces huge challenges, including restoring our trust and control over our health information. We are very concerned that neither Clinton, McCain nor Obama have responded to our Valentine's Day request to tell us where they stand on protecting our most private health records\*

**The right to protect our most sensitive information belongs at the top of the list of issues the candidates address.** Here are ways you can assess the candidates' stances and encourage them to act:

1. Consider Patient Privacy Rights' review of the 3 remaining candidates' [written records](#) on health privacy.
2. [Ask the candidates](#) to address the need for health information privacy.
3. Make sure you are [registered to vote](#) for the November 2008 election.

As you might guess, no candidate opposes our right to keep our health records private; **the right to be left alone is as American as apple pie.** However, we can point to very little action that speaks louder than words for the 3 contenders. You can click on the name of each candidate to see any remarks made or bills sponsored related to health privacy.

- [Sen. Hillary Clinton \(D\)](#)
- [Sen. John McCain \(R\)](#)
- [Sen. Barak Obama \(D\)](#)

# Consumers want privacy

## 7 Million Americans Want Privacy

The Coalition for Patient Privacy, 2008

**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.

## Privacy principles consumers want Coalition for Patient Privacy

- **Recognize that patients have the right to health privacy**
  - Recognize that user interfaces must be accessible so that health consumers with disabilities can individually manage their health records to ensure their health privacy.
- The right to health privacy applies to all health information **regardless of the source, the form it is in, or who handles it**
- Give patients **the right to opt-in and opt-out** of electronic systems
  - Give patients the right to segment sensitive information
  - Give patients control over who can access their electronic health records
- Health information **disclosed for one purpose may not be used for another purpose** before informed consent has been obtained
- Require **audit trails** of every disclosure of patient information

- Require that **patients be notified promptly** of suspected or actual privacy breaches
- **Ensure that consumers can not be compelled to share health information** to obtain employment, insurance, credit, or admission to schools, unless required by statute
- **Deny employers access** to employees' medical records before **informed consent** has been obtained
- Preserve stronger privacy protections in **state laws**
- **No secret health databases.** Consumers need a clean slate. Require all existing holders of health information to disclose if they hold a patient's health information
- Provide **meaningful penalties and enforcement mechanisms** for privacy violations detected by patients, advocates, and government regulators

## How to ensure privacy

## Privacy solutions

‘Smart’ legislation

‘Smart’ technology

- Health trusts or banks
- Independent consent management tools
- State-of-the art security

‘Smart’ certification

‘Smart’ consumers

## ‘Smart’ legislation

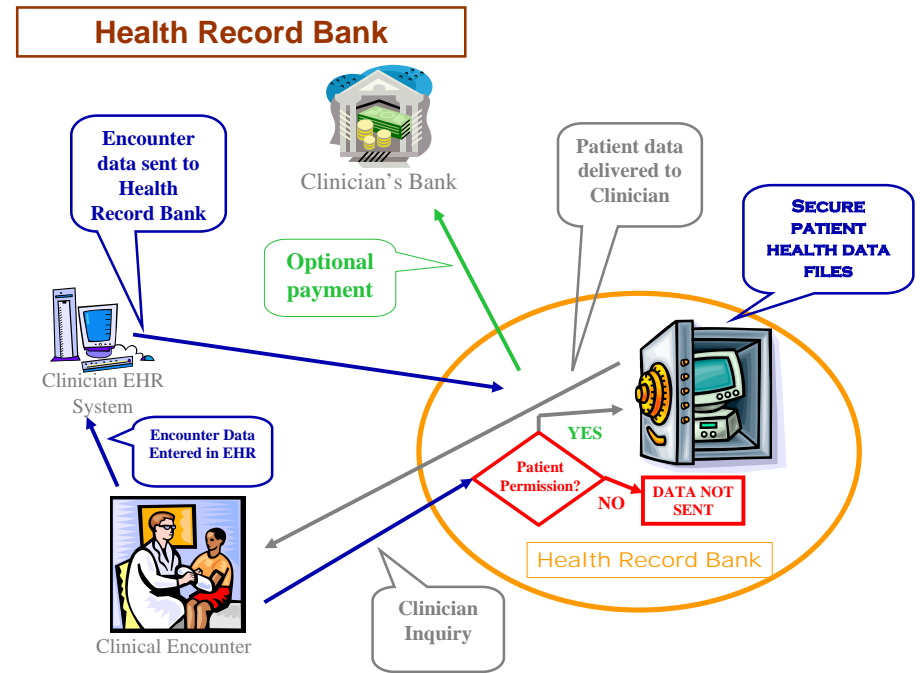
### Smart legislation - not in play

- Independent Health Record Trusts (*“Independent Health Record Trust Act of 2007”, H.R.2991*)
- TRUST Act (*“Technologies for Restoring Users' Security and Trust in Health Information Act of 2008”, H.R. 5442*)

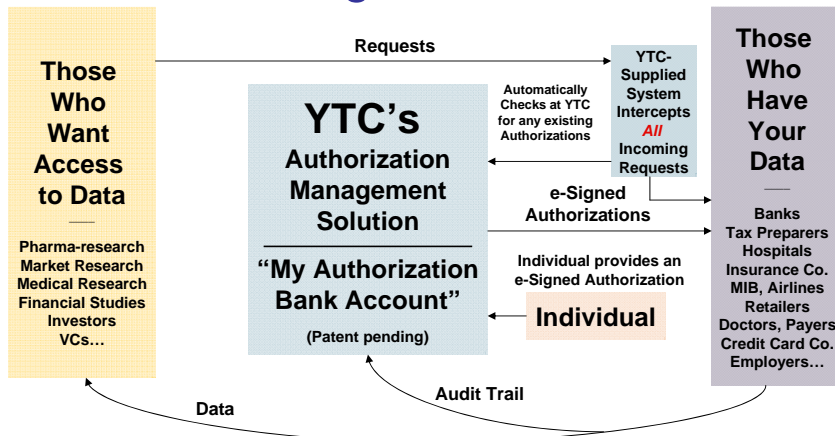


# 'Smart' technology

## Reaping the benefits of HIT with privacy



## Independent consent management tools



NOTE: YTC is the Trusted Consumer Advocate in the middle, and YTC never sees, nor stores your data

Proprietary & Confidential © 2000-2006 You Take Control, Inc.

## 'Smart' certification

## 'Smart' Certification

### PrivacyRightsCertified, Inc.

Consumer-led organization offering a Good Housekeeping Privacy Seal-of-Approval for HIT systems and products that ensure consumer control of PHI

*Privacy Rights Certified* will ensure Americans **UNDERSTAND** PHRs and EHRs, **CHOOSE** wisely, and take steps to **PROTECT** their most intimate information.

## Progress with Privacy Patient Privacy Rights

[www.patientprivacyrights.org](http://www.patientprivacyrights.org)

Deborah C. Peel, MD  
Founder and Chair

[dpeelmd@patientprivacyrights.org](mailto:dpeelmd@patientprivacyrights.org)

Ashley Katz, MSW  
Executive Director

[akatz@patientprivacyrights.org](mailto:akatz@patientprivacyrights.org)

512.732.0033 (office)

[www.patientprivacyrights.org](http://www.patientprivacyrights.org)

Will the next  
Administration restore  
privacy?

The candidates

Take Action

## Which Candidates Stand for Privacy?



Patient Privacy Rights submitted a Health Privacy [Questionnaire](#) to all Presidential candidates earlier this year. To date, we have not received responses from either candidate. We have compiled the following based on research of each candidates' record. Click on a candidate to view their Health Privacy History. Patient Privacy Rights does not endorse any candidate or party. Ask the candidates to pledge to make progress with privacy a presidential priority. Ask the candidates to pledge to make progress with privacy a presidential priority.

[http://www.patientprivacyrights.org/site/PageServer?pagename=Candidates\\_on\\_Privacy](http://www.patientprivacyrights.org/site/PageServer?pagename=Candidates_on_Privacy)



## Sen. John McCain (R-AZ) Remarks on Health Privacy:

Patient Privacy Rights could not find any specific statements about what he would do to ensure health privacy.

**Jay Khosla** McCain Advisor  
Health Counsel for the US Senate Budget Cmte(R)

10/16/08

What Senator McCain focuses on when it comes to health IT is to **make sure that we have interoperability** in the system.

What Senator McCain wants to focus on, is of course **health IT is going to need funding**.

## Policy & Legislative Record:

[Wired for Healthcare Quality Act of 2008](#), S. 1693  
(Status: pending in committee). McCain did not object to the bill's passage via unanimous consent – essentially a vote for the legislation.

McCain's website has some mention of his suggestions for healthcare reform that include lowering the cost of health insurance, making insurance more accessible and making easier for individuals to receive health insurance through means other than their employers. We did not find a clear statement supporting health IT and a national electronic health information network, or any mention of health privacy.



## Sen. Barack Obama (D-IL) Remarks on Health Privacy:

Patient Privacy Rights could not find any specific statements about what he would do to ensure *health* privacy.

## Obama third Presidential debate

“But what ultimately I believe is that women in consultation with their families, their doctors, their religious advisers, are in the best position to make this decision. And **I think that the Constitution has a right to privacy in it that shouldn't be subject to state referendum**, any more than our First Amendment rights are subject to state referendum, any more than many of the other rights that we have should be subject to popular vote.” 10/15/08

**David Cutler**      Obama Adviser  
Prof. of Applied Economics, Harvard University

10/08/08

It is my conversations with a lot of the groups of providers that have done this and the patients' groups about it suggest that people believe we can get to a point where we really do address the privacy issues and that's not a fundamental stumbling block to do it, although it is certainly something one needs to be cognisant of and make sure it's done correctly.

## Policy & Legislative Record:

[Wired for Healthcare Quality Act of 2008](#), S. 1693 (Co-Sponsor) (Status: pending in committee). Obama is a sponsor of the bill and did not object to its passage via unanimous consent – essentially a vote for the legislation.

Obama's healthcare plan: [Plan for a Healthy America](#) of 2008 includes in the Health IT portion the single statement “Obama will ensure that patients' privacy is protected.”

# Policy & Legislative Record:

According to the Obama website, in the Technology section you will find the following regarding privacy in general with some mention of health privacy specifically:

**"Safeguard our Right to Privacy:** The open information platforms of the 21st century can also tempt institutions to violate the privacy of citizens. Dramatic increases in computing power, decreases in storage costs and huge flows of information that characterize the digital age bring enormous benefits, but also create risk of abuse. We need sensible safeguards that protect privacy in this dynamic new world. *As president, Barack Obama will strengthen privacy protections for the digital age and will harness the power of technology to hold government and business accountable for violations of personal privacy.*

- Obama supports updating surveillance laws and ensuring that law enforcement investigations and intelligence-gathering relating to U.S. citizens are done only under the rule of law.
- Obama will also work to provide robust protection against misuses of particularly sensitive kinds of information, such as e-health records and location data that do not fit comfortably within sector-specific privacy laws.
- Obama will increase the Federal Trade Commission's enforcement budget and will step up international cooperation to track down cyber-criminals so that U.S. law enforcement can better prevent and punish spam, spyware, telemarketing and phishing intrusions into the privacy of American homes and computers."