

patientprivacyrights

**Do we have to choose between
privacy and health IT?**

GA Dept of Community Health HITT Advisory Board Meeting

May 16, 2007

www.patientprivacyrights.org

Why the US has no health information privacy

- Consumers don't know about the rampant secondary uses of their personal health information or how far outside the healthcare system their sensitive medical records flow
- Protections do not follow the data
- Extreme value of identifiable health data – in 2005 IMS Health made \$1.75 Billion selling prescription records

What is medical privacy?

The Original HIPAA Privacy Rules states:

“The right of privacy is: ‘the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated’.”

65 Fed. Reg. at 82,465

NCVHS Definitions of privacy, security and confidentiality

- Health information privacy - an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.
- Confidentiality - the obligations of those who receive information to respect the privacy interests of those to whom the data relate.
- Security - the physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

Letter from the National Committee on Vital and Health Statistics to Secretary of HHS, Michael Leavitt, 6/22/06.

Georgia Health Information privacy laws

- HMOs
 - May not disclose any information pertaining to diagnosis, treatment, or health without the patient's express consent. Ga. Code Ann. 33-21-23
- Physicians, Hospitals, healthcare facilities and pharmacies
 - May not be required to release any ,medical information except upon written authorization Ga. Code Ann. 24-9-40
- Insurance Entities
 - Generally may not disclose medical information received in connection with an insurance transaction without written authorization. Ga. Code Ann. 33-39-14
- Residents of long term care facilities
 - Have a right to privacy in their medical care programs. All treatment and case discussions are confidential and to be conducted in privacy. Ga. Code Ann. 31-8-114 (6)

Georgia Health Information privacy laws

- Genetic testing
 - Information is confidential and may be released only to the individual and persons authorized in writing. Ga. Code Ann. 33-54-3
- HIV/AIDS
 - A person responsible for AIDS information may not intentionally or knowingly disclose that information to another. Ga. Code Ann. 37-3-166
- Mental health records
 - May not be released without patient authorization and in several other limited circumstances. Ga. Code Ann. 37-3-166
- Privileges
 - Psychotherapist-patient privilege. Ga. Code Ann. 24-9-21
- Private right of action
 - For privacy violations by insurers, HMOs, and for improper disclosure of genetic tests. Ga. Code Ann. 33-5408

How was privacy eliminated?

- HHS eliminated the right of consent in 2002, making HIPAA a “disclosure rule”
- Over 4,000,000 health-related businesses – **including employers** - can see and use identifiable personal health information (PHI)
- Patients no longer control who sees and uses their electronic health records

HHS Amendments gutted HIPAA

1996

Congress passed HIPAA, and instructed the Dept. of Health and Human Services (HHS) to address the rights of patients to privacy.

*“Not later than the date that is 12 months after the date of the enactment of this Act, 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 original HIPAA “Privacy Rule” recognizing 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

Amendments to the “Privacy Rule” became effective eliminating “right of consent”.

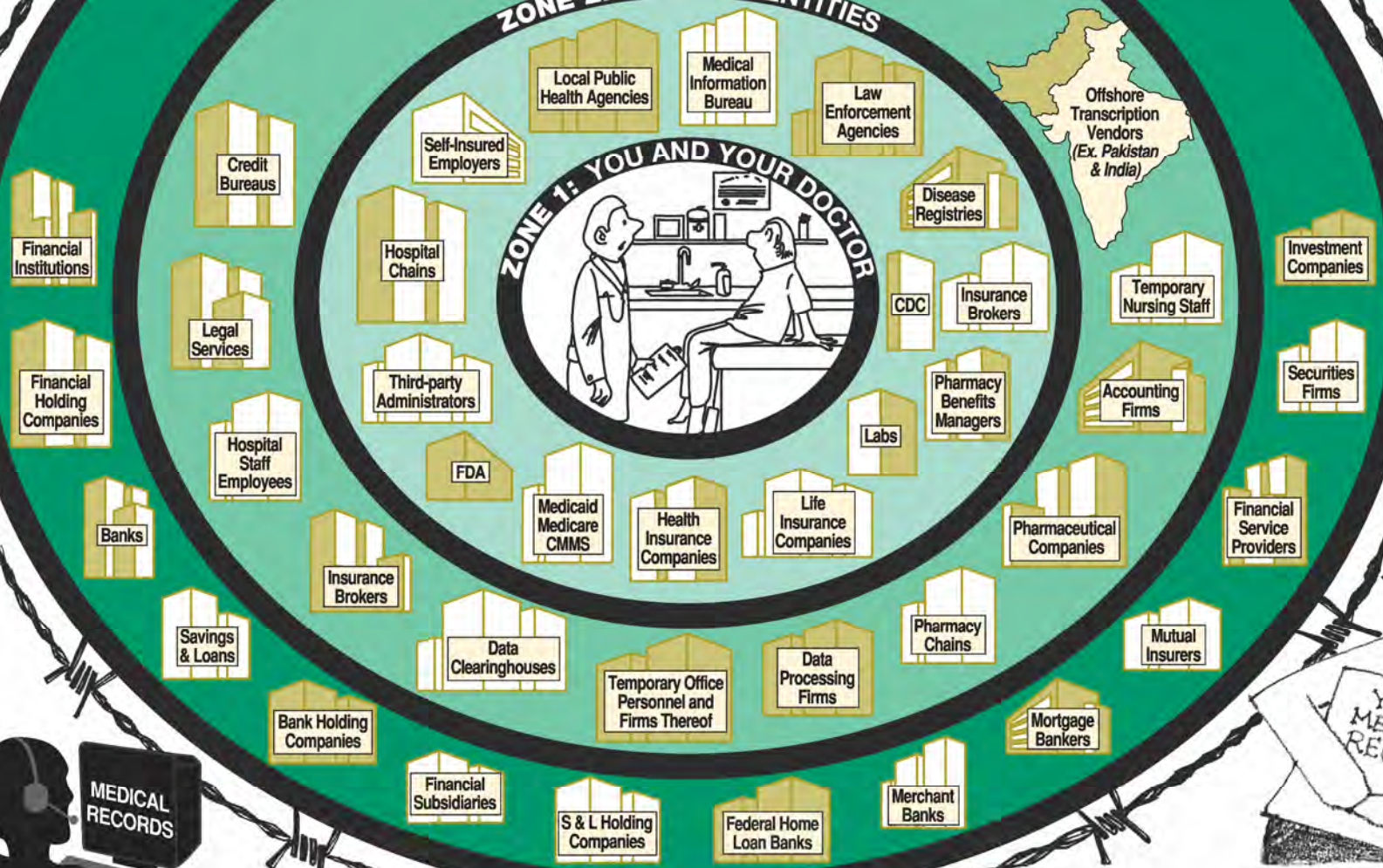
*“The **consent provisions...are replaced** with a new provision...that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations.”*

ZONE 4: GRAMM LEACH BILEY FINANCIAL SERVICES ACT

ZONE 3: BUSINESS ASSOCIATES

ZONE 2: COVERED ENTITIES

ZONE 1: YOU AND YOUR DOCTOR



Where does health information go?

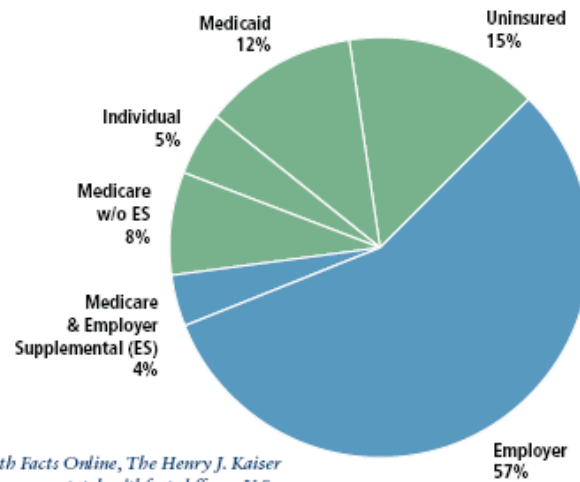
Secondary uses

- Thomson Medstat sells data from Medicare, Medicaid, health plans, and the uninsured
- BCBS sells 79 million enrollees' health records- see the Blue Health Initiative on the BCBS website
- Daily data mining of prescriptions from the nation's 51,000 pharmacies (IMS Health, Verispan LLC, others)—for insurance underwriting and physician marketing
- IRS rule allows hospital data mining of physicians' electronic records

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.

Anonymous data isn't

“It is impossible to de-identify health records”

Bill Yasnoff, MD, PhD

Senior Advisor, National Health Information Infrastructure (NHII), U.S. Department of Health and Human Services

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				

Should I use a PHR?

- They are designed to evade protective laws and ethics that protect medical records---they are NOT intended to be legal “medical records”
- Security and privacy protections are inadequate
- Financial model often is selling the data
- Designed to encourage consumers to add new valuable data

Data in a Model Health Plan PHR

Patient Information	Demographic and personal information, emergency contacts, PCP name and contact information, etc.
Family History	Possible health threats based on familial risk assessment. Includes the relationship, condition or symptom, status (e.g. active/inactive), and source of the data
Physiological Info.	Physiological characteristics such as blood type, height, weight, etc.
Subscriber Info.	Information regarding any subscribers associated with the individual (spouse, children)
Encounters	Encounter data in inpatient or outpatient settings for diagnoses, procedures, and prescriptions prescribed in association with the encounter
Medications	Medication history such as medication name, prescription date, dosage, pharmacy contact information, etc.
Immunizations	Information regarding immunizations such as vaccine name, vaccination date, expiration date, manufacturer, etc.
Benefit Information	Information regarding current insurance benefits such as eligibility status, co-pays, deductibles, etc.
Providers	Information regarding clinicians who have provided services to the individual
Facilities	Information regarding facilities where individual has received services
Health Risk Factors	Patient's habits, such as smoking, alcohol consumption, substance abuse, etc.
Advance Directives	Advance directives documented for the patient for intubation, resuscitation, IV fluid, life support, references to power of attorneys or other health care documents, etc.
Alerts - Allergies	Patient's allergy and adverse reaction information
Health Plan Info.	Used for plan to plan PHR transfer. Information about the sending and receiving plans.
Plans of Care	Any reminder, order, and prescription, etc. recommended by the care management and disease management program for the patient.

White Rows are Self-Reported Information

Yellow Rows are Systems-Populated Information

Effects of no medical privacy

- **Job loss/ denial of promotions**
 - people will be judged based on health information, not their qualifications, abilities, or experience
- **Insurance discrimination**
- **Credit denial**
- **Denial of admission to schools**
- **Create a new welfare classes of citizens who are unemployable and uninsurable**

What do consumers and patients want?

**From a
Presentation by Dr. Alan Westin
Markle Conference on Connecting
Americans to their Healthcare
Washington, DC
Dec 7-8, 2006**



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

Dr. Alan F. Westin

Professor of Public Law and Government Emeritus,
Columbia University

How Public Sees Privacy Risks and Benefits

- **When asked whether expected benefits to patients and society of EHR systems outweigh potential risks to privacy OR whether privacy risks outweigh expected benefits, privacy fears trump potential benefits:**
 - 42% feel “privacy risks outweigh expected benefits”
 - 29% feel “expected benefits outweigh the privacy risks”
 - BUT -- 29% say they are not sure...
- **Shows that the creation of a majority opinion on the risk-benefit judgment is still out there -- not yet formed**
- **Will be shaped by what EHR system developers DO and how they COMMUNICATE to patients and public**

Patient/Member Involvement -- 2

- “I would want to be given the right not to have any of my medical records entered into the new electronic record system” 21%
- “I don’t need to be notified of the change since I don’t think it will affect my relationship with my doctors and how they handle my information” 22%
- “Not sure” 17% (note the large figure here)
- While resting on low public majority awareness of EHR programs, these attitudes spell major potential trouble for EHR efforts

What is Being Done to Inform and Offer Choices?

- **Not aware of any field studies of how EHR programs are being introduced to patients or members and how new EHR-based rights are presented**
- **Not aware of patient/member surveys at EHR sites exploring how consumers react to the changes and rights policies**
- **Also not aware of any experiments with allowing patients or members the right to designate record portions not to go into the general EHR system, and if these are being studied**
- **Finally, are there any EHR programs that offer a general “opt out”? If so, are these being studied?**

A Looming Conflict?

- **Given 42+% of public feeling potential privacy risks outweigh potential EHR benefits**
- **And 60% of the public wanting advance explanations of EHR impacts and rights to choose how records used**
- **Could be a sharp bump ahead for EHR developers, as weak communications and a “just say yes” approach prevail**
- **Especially if advocacy groups expand a “STOP EHR PROGRAMS” movement, as urged by the Patients Privacy Rights Coalition**
- **Already happening in UK, where 53% of public and 52% of GPs oppose the UK national EHR plan, with an organized opposition**

Informing Can Be Done Well

- I believe every EHR program should develop and provide a Patient's Guide to Your New EHR System: For Enhanced Participation, Privacy and Security
- Customized to each EHR system; cover changes to all health care processes and information uses
- Spell out health-care advantages of new system to patients or members
- Show opportunities for greater patient participation in own health care processes and individual EHR-program choices
- Describe privacy/fair information practices rules and rights under EHR, in clear, non-HIPAA-style prose
- Outline data security program and safeguards
- Offer lively Qs and As, scenarios, and personal contacts

Implications

- **Privacy and data security remain absolutely critical issues for the national EHR effort and each individual system**
- **Majorities fear privacy risks, but adequate patient and member communications and choice options not present yet**
- **Calls for empirical field studies of the EHR introduction process, patient and member communications, and new privacy, security, and participation policies**
- **Along with surveys of patient and member perceptions, concerns, and experiences in various EHR program settings**
- **Now is the right time in EHR activities for such studies -- not too soon and not too late**

Solutions

- Build public awareness of dangers
 - secondary uses of health information
 - protections do not follow the data
- Promote ‘smart’ technology with ironclad privacy and security protections
- Educate state and federal lawmakers

Consumer Outreach

- Build a state privacy coalition and website
 - Coordinate activities and e-campaigns
 - Build a “Toolkit” to help consumers take effective action
 - Build a resource library
 - Hold conferences on privacy law and latest threats to privacy
- Contact lawmakers
 - Educate lawmakers about privacy and privacy-enhancing health IT
- Media
 - Build a list of media contacts
 - Disseminate press releases and key documents

Online General 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 Dossia 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 confirms Patient Privacy Rights' cautionary statements against PHRs.

- [See Patient Privacy Rights' summary of the ONCHIT report](#)
- [See full ONCHIT report](#)
- [See Patient Privacy Rights' press release on PHRs](#)

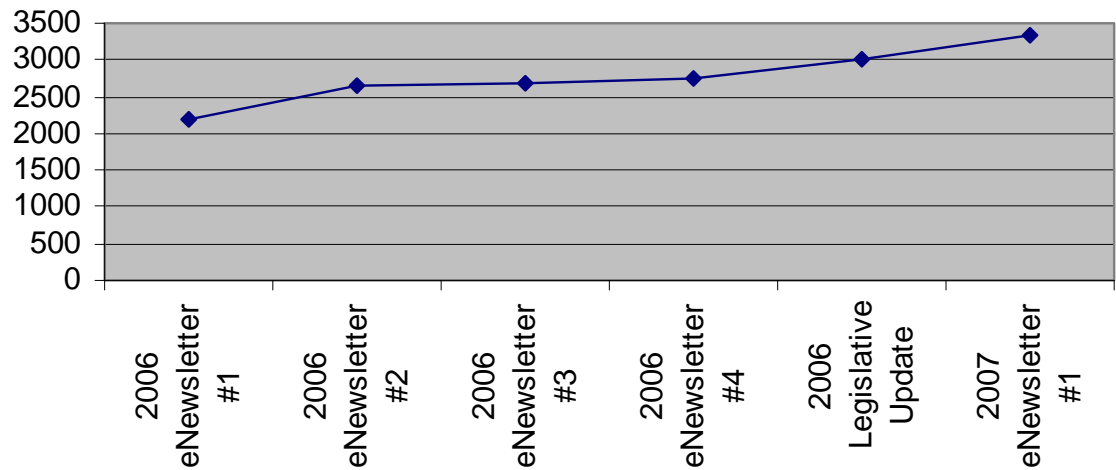
March 2007 Newsletter

In this Newsletter

- [Personal Health Records Latest Battle in Assault on Medical Privacy](#)
- [On the Congressional Agenda:](#)

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

PPR eNewsletter Audience



patientprivacyrights

Build and use on-line resources

patientprivacyrights

NEWS STORIES

We've gathered media stories about medical privacy, patient privacy violations, and healthcare information technology.

These stories are listed by date, with the most recent listed first.

[Letter: Data belongs to the patient](#)
Modern Healthcare - 4/2/07 - In response to Andis Robeznieks' article 'Health IT has potential to ease money woes', I sincerely believe that health IT has the potential to improve healthcare delivery and it would be wonderful if physicians and patients would engage the idea. Having the patient data at the point of service is everything good.

[Chasing Paper from Medicine](#)
Time - 3/30/07 - Glen Tullman didn't invent information technology, but he is one of those people who figured out early how to aim it with effect. Case in point: the 3

Top News

The Bush administration has no clear strategy to protect the privacy of patients as it promotes the use of electronic medical records throughout the nation's health care system, federal investigators say in a new report. [Read the article from The New York Times.](#)

Protect Your Privacy

First, sign the "[I Want My Medical Privacy](#)" petition today and tell Congress you want to control who sees your medical records. Then, [visit our Take Action section](#) for other steps you can take to protect your medical privacy.

- 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

Use 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 my medical privacy!
- Remember me

patientprivacyrights

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).

patientprivacyrights

- "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.

Summary: restoring medical privacy

- **Public education and media campaigns**
 - Inform and educate consumers about the loss of privacy, understanding technology and how it can provide privacy via exquisite granular control of data, education about state-of-the-art security measures
 - Build a state privacy coalition, link to other state and national medical privacy organizations
 - Hold conferences, use e-campaigns, obtain earned media
- **Identify and promote “smart” technology in the marketplace**
 - Require ‘real’ security for databases, EHRs, and PHRs: multiple layers of encryption, encryption of data at rest as well as when transmitted, PKI technology
 - Consent / authentication systems
 - Health banks controlled by consumers/patients
- **Work with state and federal agencies, and participate in public/private advisory and standards setting organizations**
 - HHS, ONCHIT, OCR, CMS, FDA, HS, CDC, AHIC, CCHIT, HITSP, HITSPC, NCVHS
 - State level RHIOs, HIEs
- **Work with Congress on federal legislation**
 - HIT bill, health banking, GINA, PHRs, stand-alone medical privacy bill
- **Join the national Coalition for Patient Privacy**
 - Bipartisan: including the Christian Coalition, the ACLU, and the California Medical Assoc.
 - In 2006 over 40 organizations urged Congress to add basic privacy protections to legislation
 - In 2007 new privacy protections are urgently---will your organization join with us?

Basic Privacy Principles

For federal HIT Legislation in 2007

- Recognize the individual's right to medical privacy
- The right to privacy should apply to all health information regardless of the source, the form it is in, or who handles it
- Give patients control over who can see & use their electronic medical records
 - **Allow opt-in, opt-out**
 - **Allow the right to segment sensitive information**
- Provide audit trails, breach notification, and meaningful penalties for privacy violations
- No coerced disclosures of health information to employers or others
- No secret data health bases
- Preserve stronger protections in state law, common law, Constitutional law

patientprivacyrights

Contact Information:

Deborah C. Peel, MD
Founder and Chair
Patient Privacy Rights Foundation

PO Box 248
Austin, TX 78767

512.732.0033 (office)

dpeelmd@patientprivacyrights.org
www.patientprivacyrights.org