4th Annual Government Health IT Conference

Privacy and Health IT:
Establishing Reliable and Practical Approaches

PROGRESS WITH PRIVACY

Friday, June 13, 2008

Deborah C. Peel, MD

patientprivacyrights

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

Forrester Research

an independent technology and market company that provides advice to global leaders in business and technology

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?

Privacy means control over personal information.

Without control, you have no privacy.

Overview

- Why should you care about privacy?
- What is happening in the market?
- Why can’t we rely on HIPAA to protect privacy?
- What is happening in Congress?
- How to ensure privacy and quality

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)

Quality without Privacy?

The Institute of Medicine's (IOM) definition of quality health care includes six quality improvement measures:

safety, effectiveness, patient-centeredness, timeliness, efficiency, and equity

But NOT privacy

Without Privacy, Quality Suffers

- The **entire health delivery system** is based upon the willingness of the individual to trust a health care practitioner sufficiently to disclose to the practitioner the most intimate details of his or her life.
- An assurance of privacy of health information is **necessary to secure effective, high quality health care.**

65 Fed. Reg. at 82,467.

IOM Survey: People Won't Trust Research Without Privacy

by Dr. Alan F. Westin, October 2, 2007

- 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.

“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.”

Unintended consequences

Increases costs

- Delayed treatment

Decreases quality

- Suffering
- Deaths
- Absent or limited data

Poor quality research

- People fear participation

Unintended consequences

Decreases competition

- HIT vendors can't compete by offering individuals more control

No transparency

- Without audit trails, you will never know where your data flows or how many secret data bases exist with your PHI

Other Consequences

Employers Discriminate

- **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)*

Wal-Mart Memo Suggests Ways to Cut Employee Benefit Costs

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

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

The New York Times

The New York Times

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.

Consequences of no control over your PHI:

- **Job loss/ denial of promotions**
  - People are judged on health information, not qualifications, abilities, or experience
- Insurance discrimination
- Credit denial
- Denial of admission to schools
- Marketing
- *New classes of citizens who are unemployable and uninsurable*

What is Happening in the Market?

Electronic Health Systems~

Not Ready for Primetime

EHRs and PHRs: Weak Security, No privacy, Secondary Uses

Weak security

- Easy to hack from the outside
- No role-based access, i.e., no consumer access controls (hacking from the inside)

No privacy

- Over 4 million providers can access protected health information (PHI) for treatment, payment, and healthcare operations (TPO)

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)

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.

EMR vendor to share patient data with genetics research firm

Healthcare IT News, 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.”

HealthcareITNews

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."***


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

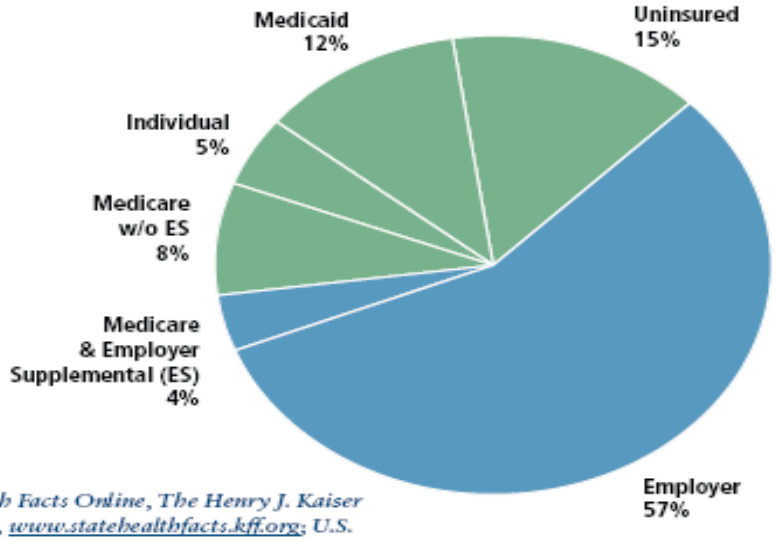
Personal health information is for sale

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				

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.

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."

HIPAA does NOT Protect Privacy

Elimination of Consent

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.

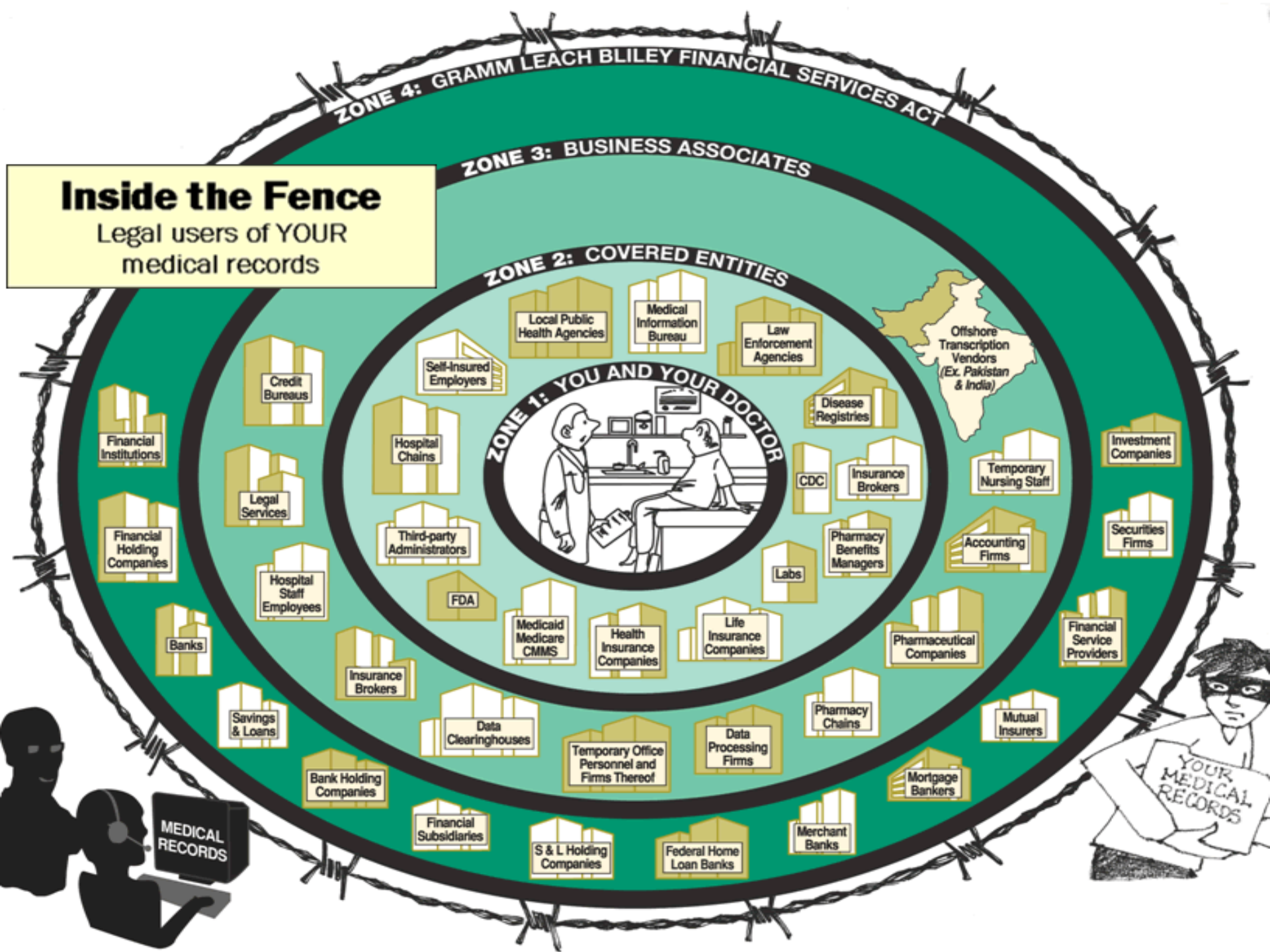
> *"… the Secretary of Health and Human Services shall submit to [Congress]…**detailed recommendations on standards with respect to the privacy of individually identifiable health information."***

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."*


ZONE 4: GRAMM LEACH BLILEY FINANCIAL SERVICES ACT
ZONE 3: BUSINESS ASSOCIATES
ZONE 2: COVERED ENTITIES
ZONE 1: YOU AND YOUR DOCTOR
Inside the Fence
Legal users of YOUR medical records
Local Public Health Agencies
Medical Information Bureau
Law Enforcement Agencies
Offshore Transcription Vendors (Ex. Pakistan & India)
Self-Insured Employers
Credit Bureaus
Financial Institutions
Hospital Chains
Disease Registries
Investment Companies
Legal Services
CDC
Insurance Brokers
Temporary Nursing Staff
Financial Holding Companies
Third-party Administrators
Pharmacy Benefits Managers
Securities Firms
Hospital Staff Employees
Accounting Firms
Labs
FDA
Medicaid Medicare CMMS
Health Insurance Companies
Life Insurance Companies
Pharmaceutical Companies
Financial Service Providers
Banks
Insurance Brokers
Savings & Loans
Data Clearinghouses
Pharmacy Chains
Mutual Insurers
Temporary Office Personnel and Firms Thereof
Data Processing Firms
Bank Holding Companies
Mortgage Bankers
Financial Subsidiaries
S & L Holding Companies
Federal Home Loan Banks
Merchant Banks
MEDICAL RECORDS
YOUR MEDICAL RECORDS

HIPAA Allows Identifiable Data Mining

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.

Health Privacy Project 2002

This proposal [by HHS] to eliminate the consent requirement strikes at the very heart of the Privacy Rule and takes away a core privacy protection for consumers.

The Privacy Rule's consent requirement is the best way to ensure that patients actually know how their health information is used and what their privacy rights are.

Health Privacy Project 2002

It is clear that without a prior consent requirement patient will have no control over how their health information is used and disclosed beyond the right to request a restriction.

The Department's proposal to eliminate the consent requirement represents a huge step backwards for consumers and one that will undermine trust in the health care system.

Comments by Janlori Goldman filed on behalf of the Health Privacy Project on the proposed Amended Rule on April 26, 2002.

What is Happening in Congress?

‘Smart’ Legislation

- **Bipartisan Coalition for Patient Privacy**
  - 2007 privacy principles
- **Health Banking legislation**
  - Independent Health Record Trust Act, HR 2991
- **HIT legislation**
  - TRUST Act (Technologies for Restoring Security and Trust), HR 5442 introduced Feb 14, 2008

7 Million Americans Want Privacy

The Coalition for Patient Privacy, 2007

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.

2007 Privacy Principles

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

2007 Privacy Principles

Coalition for Patient Privacy

- 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

NOT part of the Solution

Legislation without privacy

- House E&C draft (Dingell, Barton, Pallone, Deal)
  - Mark-up June 18th
- Senate “Wired for Healthcare Quality Act” S 1693
  - and House companion “Promoting Health Information Technology Act” HR 3800
- e-prescribing: (E-MEDS) the Medicare Electronic Medication and Safety Protections Act of 2007
  - S 2408 (Kerry) and HR 4296 (Schwartz)

How to Ensure Privacy

Smart Solutions

‘Smart’ Legislation

‘Smart’ Technology

- Health Trusts or Banks
- Independent Consent Management Tools
- State-of-the art security

‘Smart’ Certification

Trusted 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.

Forms

- Consent Form: to give all providers **NEW!**
- How to Talk to Your Doctor
- Opt out of the AMA Database: to give all Providers **NEW!**
- Checklist: Manage your Consents **NEW!**
- Request Your Records **NEW!**
- Complaint Form to HHS

Information

- Your Health Privacy Rights
- How Marketers CAN Use Your PHI **NEW!**
- 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)
- Which Candidates stand for Privacy?
- Congress Needs to Hear from You
- Share Your Story

3 Things You Can Do Now

- Sign up for e-Alerts
- Tell Congress: "*Don't pass health IT legislation unless my control over access to my health records is restored*"
- Use the Patient Privacy Tool Kit, ask providers to sign *your* privacy forms

www.patientprivacyrights.org

DR. DEBORAH PEEL

> FOUNDER AND PRESIDENT

PATIENT PRIVACY RIGHTS

> AUSTIN, TEXAS

Progress with Privacy:
Join Patient Privacy Rights

www.patientprivacyrights.org

Deborah C. Peel, MD
Founder and Chair
dpeelmd@patientprivacyrights.org

Ashley Katz, MSW
Executive Director
akatz@patientprivacyrights.org

512.732.0033 (office)