

Institute for Behavioral Health Informatics

Plenary Keynote Address

**Privacy and Confidentiality Concerns in the
Nationwide Health Information Network**

Deborah C. Peel, MD

Thursday October 26th, 2007

patientprivacyrights

Informal Poll Results

Should ANY person or entity be able to view and use your health records WITHOUT your explicit consent?		
answer options	Response Percent	Response Count
Yes	1.08%	4
No	83.06%	309
Depends (please specify)	16.67%	62
<i>answered question</i>		372
<i>skipped question</i>		4

Informal Poll Results

What people or organizations should be able to access your personal health records WITHOUT your consent? Select all that apply or "None".		
answer options	Response Percent	Response Count
NONE	76.11%	274
City Health Agencies	1.67%	6
Data Miners	0.56%	2
Drug Companies	0.56%	2
Employers	0.28%	1
Federal Agencies	1.67%	6
Hospital Staff	12.22%	44
Insurers	3.06%	11
Pharmacies	3.61%	13
Physicians	19.44%	70
Researchers	2.22%	8
State Agencies	1.11%	4
Strangers/Hackers	0.28%	1
<i>answered question</i>		360
<i>skipped question</i>		16

Informal Poll Results

Would you use an online electronic health record, such as a PHR (Personal Health Record)?		
answer options	Response Percent	Response Count
Yes	9.04%	32
No	33.05%	117
Only if I knew I controlled the information	57.91%	205
<i>answered question</i>		354
<i>skipped question</i>		22

Premises

- **The common good, advancing the quality of health care through research is *only* possible with privacy**
- 30-40% of people with Depression or addictive Disorder get care 'off-the-grid'---they pay out-of-pocket for therapy or go to AA or NA. **Without privacy, we will never get accurate data on mental illness or accurate studies on behavioral health treatment.**
- Transparency and 'data stewardship' will not reassure individuals that their privacy is protected. Controlling all access to electronic health records, ie real consumer empowerment, is the only way individuals trust that their privacy is protected.
- 'Smart' technologies and 'smart' legislation that ensure consumers control personal electronic health records are the only route to HIE and accurate research data

patientprivacyrights

- The public has no idea how much research occurs today without consent (research, QI, registries, PH, private research corporations, hospital reviews, CMS, MCOs, JCAHO, PBMs, etc, etc)
- The public has no idea how many thousands of databases are being built with their PHI—many are justified as being useful ‘for research’ (BHI, Rx databases, Thomson Medstat, etc)
- There has been no public debate on access to PHI and ‘secondary’ uses or ‘onward transfer’ of data without consent
- Awareness of the lack of privacy and poor security in electronic health systems is increasing
- Researchers do not all have the same degree of public confidence (Mayo vs. drug industry)

patientprivacyrights

Overview

Today health privacy does not exist—
'secondary' uses are the **primary** uses
of Americans' personal health
information

“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

patientprivacyrights

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
- HIPAA eliminated consent
- Coerced illegal consents (Rothstein article in JAMA)
- Data worth billions to insurers, to employers, to drug industry – in 2005 IMS Health made \$1.75 Billion selling prescription records
- Protections do not follow the data

patientprivacyrights

The Elimination of Consent

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.”*

patientprivacyrights

Inside the Fence

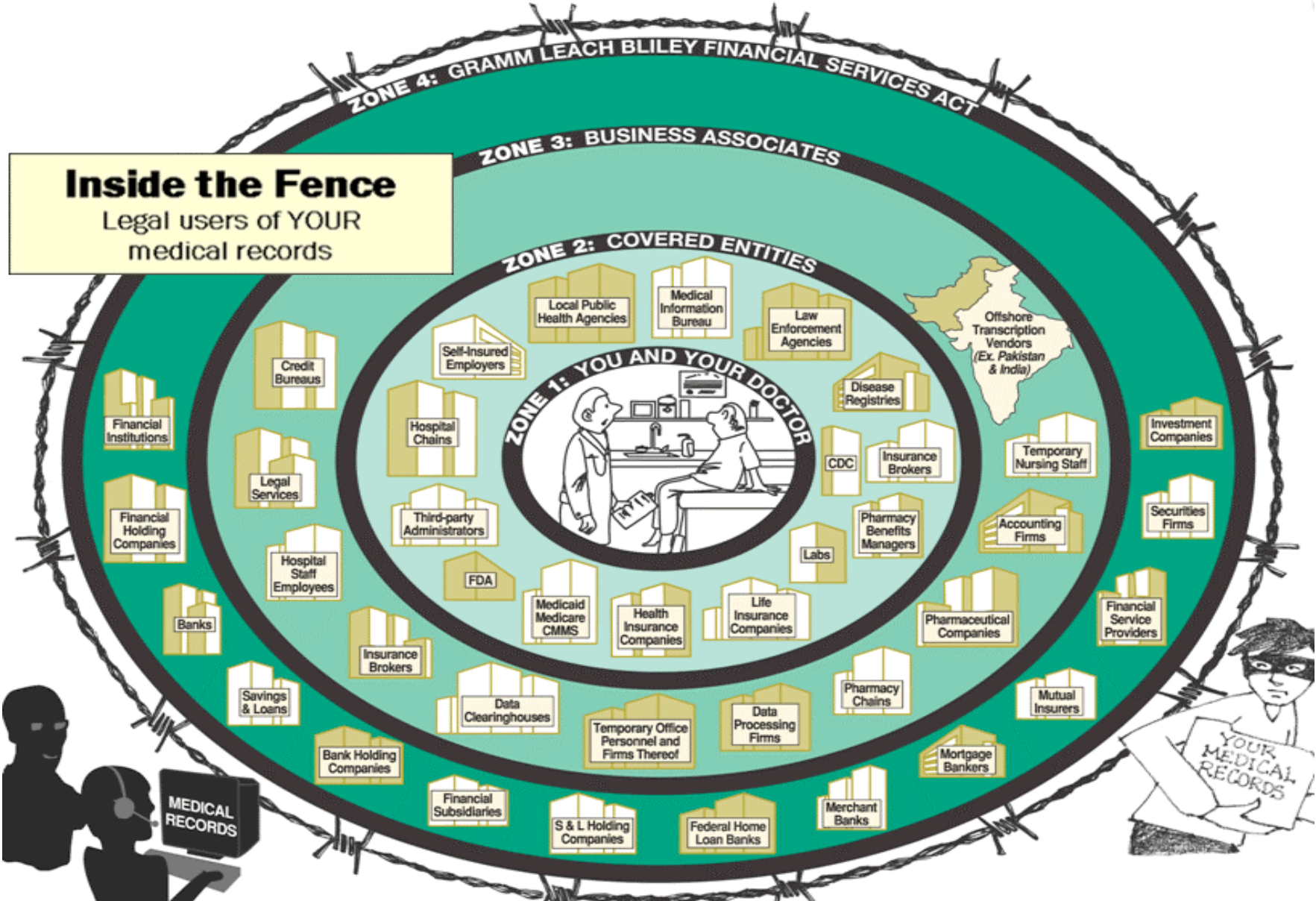
Legal users of YOUR medical records

ZONE 4: GRAMM LEACH BLILEY FINANCIAL SERVICES ACT

ZONE 3: BUSINESS ASSOCIATES

ZONE 2: COVERED ENTITIES

ZONE 1: YOU AND YOUR DOCTOR



patientprivacyrights

Effects of no medical privacy

- 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
- New classes of citizens who are unemployable and uninsurable

patientprivacyrights

What Does the Public Expect?

- Polls show the expectation of privacy and security, fear of electronic systems
- Laws should protect consumers' rights
- Ethics should prevail

patientprivacyrights

Consumer Polls

67% of Americans are concerned about the privacy of their personal medical records--recent privacy breaches have raised their level of concern

- *24% are aware of specific breaches where PHI was compromised*
- *66% say they are more concerned about their medical records as a result*

1 in 8 Americans have put their health at risk by engaging in privacy-protective behavior:

- *Avoiding their regular doctor*
- *Asking a doctor to alter a diagnosis*
- *Paying privately for a test*
- *Avoiding tests altogether*

52% said they were concerned that insurance claims information might be used by an employer (an increase of 44% from the 1999 study)

CHCF Consumer Health Privacy Survey 2005

patientprivacyrights

Consumer Polls

Three-quarters of the public want the government to set rules to protect the privacy and confidentiality of electronic health information.

Two-thirds want the government to set rules controlling the secondary uses of information

Markle Foundation Survey, November 2006

66% of Americans believe Congress should make protecting information systems and networks a higher priority. Of that group, 46% said they would have “serious” or “very serious” doubts about political candidates who do not support quick action to improve current laws.

Federal Computer Week, May 23, 2006

Most Americans are “highly concerned” about the privacy of their health information.

UPI Poll: Concern on Health Privacy, February 21, 2007

patientprivacyrights

Consumer Polls

62% to 70% of Americans are worried that sensitive health information might leak because of weak data security; that there could be more sharing of patients' health information without their knowledge; that computerization could increase rather than decrease medical errors; that some people won't disclose necessary information to healthcare providers because of worries that it will be stored in computerized records; and that existing federal health privacy rules will be reduced in the name of efficiency.

Testimony of the Markle Foundation before the Senate Committee on Homeland Security and Governmental Affairs, February 1, 2007

42% of Americans feel that “privacy risks outweigh expected benefits” from health IT. Harris/Westin poll on EHRs and Privacy (2006).

patientprivacyrights

Consumer Polls re: Research

*The public only supports use of their electronic personal health information for purposes other than their treatment **with appropriate safeguards**.*

A majority of Americans would be willing to share their information **with their identity protected** for:

- for public health to detect disease outbreaks (73%)
- bio-terrorist attacks (58%)
- with researchers, doctors, and hospitals to learn how to improve quality of care(72%)
- to detect medical fraud (71%)

But *most Americans want to have control over the use of their information for these purposes.*

Markle Foundation Survey, November 2006

patientprivacyrights

Consumer Polls re: Research

38% of Americans want researchers to first describe the study and get specific consent before using PHI (represents 85.5M)

16 groups were higher than the 38% in wanting notice and consent:

- Black 45%
- College grad 46%
- 35K-49K 45%
- 50-64 43%
- Single women 43%
- Very informed/study 51%
- Very comfortable/study 49%
- Long-term health condition 45%
- Used mental health services 44%
- Sexual condition 49%
- Had genetic test 48%
- High interest interest in research 46%
- Participated in study 44%

Survey Findings on Health Research
Dr. Alan F. Westin for the IOM, October 2, 2007

patientprivacyrights

Consumer Polls re: Research

Major Implications of the Westin/Harris IOM survey:

- 4/10 (representing 88.5M out of 255M) adults in the US insist on notice and express consent
- Many crucial groups have higher rates insisting on consent and notice
- Research using EHR systems, online PHRs, disease-based data bases, and registries is not blindly supported

Survey Findings on Health Research
Dr. Alan F. Westin for the IOM, October 2, 2007

patientprivacyrights

Constitutional Protections

Federal courts have found consistently that the right to informational privacy, as *distinct from the right to decisional privacy*, is protected by the Fourteenth, Fifth and Fourth Amendments to the United States Constitution. Whalen v. Roe, 97 S. Ct. 869, 877 (1977); Ferguson v. City of Charleston, 121 S. Ct. 1281, 1288 (2001)

“The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with non-medical personnel without her consent.”; U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dodds, 419 F.3d 1097 (10th Cir. 2005).

In fact, *the constitutionally protected right to privacy of highly personal information is so well established that no reasonable person could be unaware of it.* Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000).

patientprivacyrights

Legal Privileges

A physician-patient privilege is recognized in the laws of 43 states and the District of Columbia.

The State of Health Privacy, Health Privacy Project (2000)

A psychotherapist-patient privilege is recognized in the laws of all 50 states and the District of Columbia.

Jaffee v. Redmond, 116 S. Ct. 1923, 1929 (1996)

patientprivacyrights

Common Law

All 50 states and the District of Columbia recognize in tort law a common law or statutory right to privacy of personal information.

HHS finding 65 Fed. Reg. at 82,464

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

patientprivacyrights

Ethics Protect Health Privacy

“Privacy and confidentiality [of health information] are neither new concepts, nor absolutes. ***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).

The right to not have health information disclosed without consent is reflected in the Hippocratic Oath dating from the 5th Century B. C. which is taken by most medical school graduates and in the standards of professional ethics adopted by virtually every segment of the medical profession. 65 Fed. Reg. at 82,472; The Use of the Hippocratic Oath: A Review of 20th Century Practice and a Content Analysis of Oaths Administered in Medical Schools in the U.S. and Canada in 1993, R. Orr, M. D. and N. Pang, M. D.

patientprivacyrights

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.

patientprivacyrights

Where does health information go?

- **Thomson Medstat sells data from Medicare, Medicaid, health plans, and the uninsured**
- **BCBS sells all 79 million enrollees' health records-** In 2006, Blue Cross and Blue Shield touted the nation's largest database of consumer health data as providing "a treasure trove of information that employers working with health plans can use to extract greater value for their health care dollars."

BCBS' Medical Director David Plocher, MD, 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." Further he said that he was "very enthralled about the ability to help multi-state employers fix their healthcare costs." During the one and one-half years that BCBS has been building the BHI database, he had "never heard about privacy concerns."

- **Daily data mining of prescriptions from the nation's 51,000 pharmacies** (IMS Health, Verispan LLC, others)—for insurance underwriting and physician marketing
- **New IRS rule allows hospital data mining of physicians' electronic records**

patientprivacyrights

Secondary Users/Sellers

- Rx Switching companies, PBMs
- Technology Industry (via vendor contracts)
- Insurance Industry
- Data aggregators and data miners
- Hospital industry
- Transcription industry
- Banks and the financial industry (via GLB)
- Self-insured employers
- Data management corporations

patientprivacyrights

Unknown Secondary Uses for Research

- Quality Assurance/Improvement, hospital-based studies
- Research using medical records without consent (Privacy Act or IRB approved)
- State and Federal databases and registries
- Some Public health uses
- Private research corporations, MCOs, PBMs
- CMS, JCAHO, etc

patientprivacyrights

FDIC Notice April 28, 2004

MEDICAL PRIVACY REGULATIONS UNDER THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003

Except as permitted by the appropriate regulators, **section 411 prohibits creditors from obtaining or using medical information to make credit determinations.** Except as permitted by the regulators or the FACT Act itself, **section 411 treats medical information as a credit report when a creditor shares it with an affiliate.** The attached notice of proposed rulemaking proposes the exceptions to section 411 that will be permitted by the regulatory agencies.

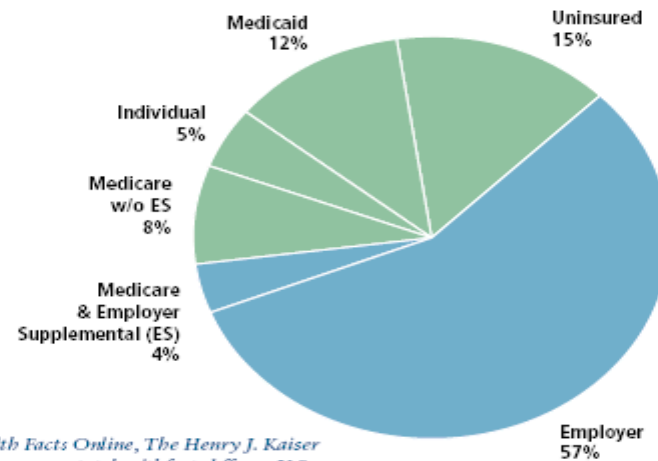
First, **section 411 states that a creditor may not obtain or use a consumer's medical information, as defined in the Act, in connection with a determination of a consumer's eligibility, or continued eligibility, for credit.** The statute itself contains no exceptions to the prohibition, but requires that the regulatory agencies publish rules setting forth those exceptions "determined to be necessary and appropriate to protect legitimate operational, transactional, risk, consumer, and other needs." Second, **section 411 states that when affiliates share certain medical information, that information will be considered a consumer report under the FCRA.** Section 411 sets forth certain exceptions, but authorizes the regulatory agencies to draft additional exceptions for entities under their respective jurisdictions.

patientprivacyrights

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.

patientprivacyrights

Anonymous data *isn't*

“... a common practice is for organizations to release and receive person specific data with all explicit identifiers, such as name, address and telephone number, removed on the assumption that anonymity is maintained because the resulting data look anonymous. However, in most of these cases, the remaining data can be used to re-identify individuals by linking or matching the data to other data or by looking at unique characteristics found in the released data.”*

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

*k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10 (5), 2002; 557-570.

patientprivacyrights

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				

patientprivacyrights

PHRs: Designed for Data Mining

- The laws and ethics protecting medical records do not apply to PHRs
- Security and privacy protections are inadequate
- Financial model often is selling the data
- Consumers are encouraged to add valuable new data to PHRs that can be data mined
- Review of the Personal Health Record (PHR) Service Provider Market, Privacy and Security, January 5, 2007
 - Conclusion: “Based on our analysis of 30 PHR vendors, existing privacy policies are incomplete.”
 - The report was developed for the Office of the National Coordinator for Health Information Technology (ONC) by Altarum Institute.

patientprivacyrights

Solutions and Conceptual Framework

- Smart Consumers
- Smart Technology
- Smart Legislation

patientprivacyrights

Smart Consumers

Only individual consumers can strike the “balance” between personal privacy and all secondary uses of PHI

- 2007 Privacy Principles developed by the Coalition for Patient Privacy
- Longstanding legal and ethical rights to privacy

patientprivacyrights

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

patientprivacyrights

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

patientprivacyrights

Smart Technology

- Smart Privacy
 - independent consent management tools control access to all PHI
 - independent health record trusts hold complete, lifetime PHI
- Smart Security
 - state-of-the-art physical and technical standards
 - data encryption at rest and in transit
 - strong 2-factor authentication of users
 - PKI
 - firewalls
- Smart protections ensure privacy and security **while** ensuring access to the right data, at the right time and place
 - Limit releases of PHI, because it is impossible to de-identify. Research, studies, and queries should be run by health records trusts if consumers consent to participate
 - annual privacy and security audits of all systems and products

patientprivacyrights

Smart Technology

Microsoft's HealthVault <http://www.healthvault.com/>

- ***new 'best practices' standard for health IT industry***
- ***consumers totally control PHI***
- only email address required, no name/ID, can have pet accounts
- adheres to the 2007 principles of Coalition for Patient Privacy
- cannot be data-mined (technically or contractually)
- all onsite Partners must meet same high privacy standards
- independent third-party audits prove compliance with privacy principles
- no secondary use of data without explicit informed consent
- onsite advertisers may only use data for the purpose advertised
- safe searches onsite (information brought inside, no tracking)
- ***proof privacy works in the 'real' world***

patientprivacyrights

Smart Legislation

- ***Congress should restore our health privacy rights***

See Oct 18, 2007 Coalition for Patient Privacy's letter to Congress

http://www.patientprivacyrights.org/site/DocServer/Letter_to_Congress_Final_10_17.07.pdf?docID=2281

- ***HIPSA***

(Kennedy-Leahy "Health Information Privacy and Security Act", S.1814)

- **Independent Health Record Trusts**

("Independent Health Record Trust Act of 2007", H.R.2991)

patientprivacyrights

Health Record Trusts

- Cradle-to-grave PHI is stored in a Health Record Trust (IHRT) account
- Patient (or designee) controls all access to account information [copies of original records held elsewhere]
- When care received, new records sent to IHRT for deposit in patient's account
- All data sources must contribute PHI at patient request (per HIPAA)

patientprivacyrights

Secondary Uses via Consent and Trusts

- Independent consent management tools ensure privacy
- Health record trusts facilitate desired secondary uses
 - Searches over large populations is easy
 - Not necessary to release PHI
 - Counts of matches with demographics normally sufficient
 - Eliminates issues of “de-identification” and reuse
 - Can combine searches over multiple trusts
 - Consumers are notified of studies without knowledge of researchers (e.g. for clinical trial recruitment, drug withdrawal from market) via trust

patientprivacyrights

Danger/Opportunity

- These are dangerous times for privacy:
 - The Administration, HHS, ONCHIT, HITSP, CCHIT, AHIC, NCVHS, IOM, etc are rushing ahead to build HIT without privacy
 - Congress: Senators Kennedy, Clinton, Hatch, Enzi, and 7 other co-sponsors of the “Wired for Health Quality Act” of 2007, S. 1693 are pressing for passage of this bill without meaningful privacy protections. Eshoo recently introduced the House companion bill, the “*Promotion of Health Information Technology (HIT) Act*”, H.R. 3800
- These are opportune times for privacy:
 - The largest technology corporation in the world agrees that privacy is essential---the market is moving far ahead of Congress
 - Microsoft’s actions set a new high bar for HIT privacy and will inevitably require all HIT products and systems to put consumers in control of PHI (including EHR systems, claims data, lab data, genetic test results, prescriptions, and hospital systems)
 - Public worry about risks of HIT is growing

patientprivacyrights

Call to Action

Be a 'smart' institutional leader

- Design or purchase HIT systems that meet the new high bar for privacy set by Microsoft's HealthVault
- Adhere to tough privacy principles, proven compliance via audits
- Collaborate with experts in consumer health privacy organizations
- Use ethical HIT systems---the ones consumers will choose

patientprivacyrights

Be a 'smart' consumer

- Stay informed at www.patientprivacyrights.org (sign up for e-alerts and news)
- Contact your lawmakers about restoring your right to privacy
- Ask other state and national organizations to join the Coalition for Patient Privacy
- Download forms to take to providers and assert your privacy rights
http://www.patientprivacyrights.org/site/PageServer?pagename=Right_To_Medical_Privacy_Statement&JServSessionIdr009=91n5w20hw1.app8b
- Help us today! Please donate to PPR at:
<http://www.patientprivacyrights.org/site/PageServer?pagename=Donate>

patientprivacyrights

A STATEMENT OF MY RIGHT TO MEDICAL PRIVACY

PLEASE PLACE COPIES IN MY MEDICAL AND BILLING RECORDS

I assert my right of consent as codified in common law, the laws of this state, and in the traditional ethical principles governing medical privacy embodied in the American Medical Association's Code of Medical Ethics. I do not agree to any disclosures of any part of my medical records or my family's medical records without my specific consent.

Patient signature

Date_____

Please indicate below whether you agree or refuse to obtain my express consent before disclosing my health information or my family's health information.

____ I agree to disclose your health information only with your express consent.

____ I do not agree to obtain your express consent before disclosing your health information.

Treating Provider (or privacy officer, administrator)

Date_____

Contact Information

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

Ashley Katz, MSW
Executive Director
Patient Privacy Rights Foundation

512.732.0033 (office)

www.patientprivacyrights.org

patientprivacyrights