The Fifteenth National HIPAA Summit:

Advocating for Patient Privacy Rights

The "P" in HIPAA does not stand for "Privacy"

Deborah C. Peel, MD

Friday December 14, 2007

patientprivacyrights

Today's landscape

Health privacy simply does not exist–illegal and unethical "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."

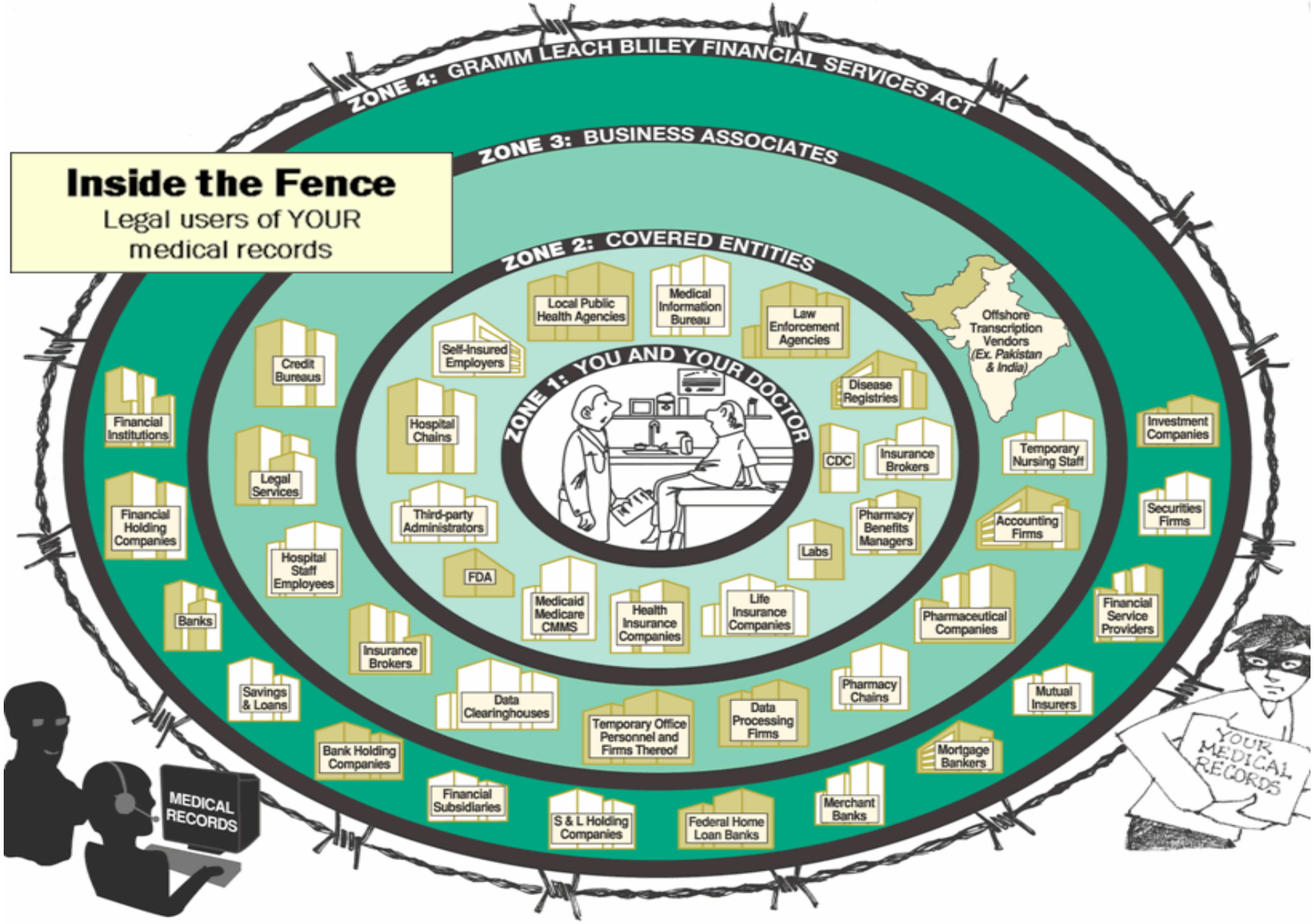
Forrester Research

Why the US has no health information privacy

- **HIPAA eliminated consent**
- Widespread use of coerced illegal consents
  (**Compelled Disclosure of Health Information - Protecting Against the Greatest Potential Threat to Privacy**, *Wednesday, June 28, 2006, JAMA.*2006; 295: 2882-2885 *By: Mark A. Rothstein, JD Meghan K. Talbott, JD)*
- Protections do not follow the data
- 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—BCBS' Blue Health Initiative; Rx databases such as IMS Health, Verispan LLC, and NEPSI (the National ePrescribing Patient Safety Institute), Thomson Medstat, McKesson, etc
- Data worth billions to insurers, to employers, to drug industry – in 2005 IMS Health made $1.75 Billion selling prescription records

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."*



www.patientprivacyrights.org

Compliance and propaganda —
what do consumers *really* want?

HIPAA does NOT protect our privacy —
The devil's in the details of the so-called "Privacy Rule"

Solutions to create trusted electronic health systems —
"smart" technology and "smart" laws

The Future

- Public awareness of the lack of privacy and poor security in electronic health systems will only **increase**
  - *Oct. 2007 - Just 10 minutes on an afternoon cable show: phones ringing off the hook, thousands of hits to website*
- Vendors that build **consumer control** of access to PHI into HIT products and systems will win in the marketplace

What do consumers really want?

- Privacy and security in electronic health systems
- Laws that protect consumers' rights
- An ethical healthcare system

What is the Privacy Problem?

- '*Compliance with HIPAA*' or *being a 'covered entity*' does not reassure Americans that their privacy is protected (Westin-Harris survey Oct '07).
- *Real* consumer empowerment is control over all access to PHI
- Consumers won't participate in HIT/HIE systems unless ironclad privacy rights are built in. Consumers won't trust anything else.
- 'Smart' technologies that ensure consumer control of personal electronic health records are the only route to HIE.

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

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

Consumer polls

62% to 70% of Americans are worried:

- sensitive health information might leak because of ***weak data security***
- there could be ***more sharing of patients' health information without their knowledge***
- *computerization could increase* rather than decrease *medical errors*
- people won't disclose necessary information to providers because of worries that it will be stored in computerized records;
- ***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

Consumer polls

42% of Americans feel that "*privacy risks outweigh expected benefits*" from health IT.

Harris/Westin poll on EHRs and Privacy (2006)

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

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

Consumer Polls

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

Consumer Polls

“The privacy of personal medical records and health information is not protected well enough today by federal and state laws and organizational practices.”

- 58% agree
- 42% disagree

Only a few demographic variations in the “Agree” camp

- Age 65+--66%
- In Fair Health--64%;
- Had genetic test--67%

The HIPAA Privacy Rule and its enforcement does not seem to have given a national majority much confidence in national health privacy protection

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

Constitutional protections

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).

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).

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)

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.

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 or 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.

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

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 (McKesson, IMS Health, Verispan LLC, others)—for insurance underwriting and physician marketing**
- **New IRS rule allows hospital data mining of physicians' electronic records**

Secondary users/sellers

- Rx Switching companies, PBMs
- Technology Industry (via vendor contracts)
- Insurance Industry
- Data aggregators and data miners
- Hospitals
- Transcription industry

Secondary users/sellers

- Banks and the financial industry (via GLB)
- Self-insured employers
- Data management/aggregation industry
- Quality assurance/improvement, hospital-based studies
- Research without consent (via Privacy Act, IRB, or Privacy Board approvals)
- State and federal databases and registries
- Public health uses

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.

Personal health information is for sale

THOMSON MEDSTAT

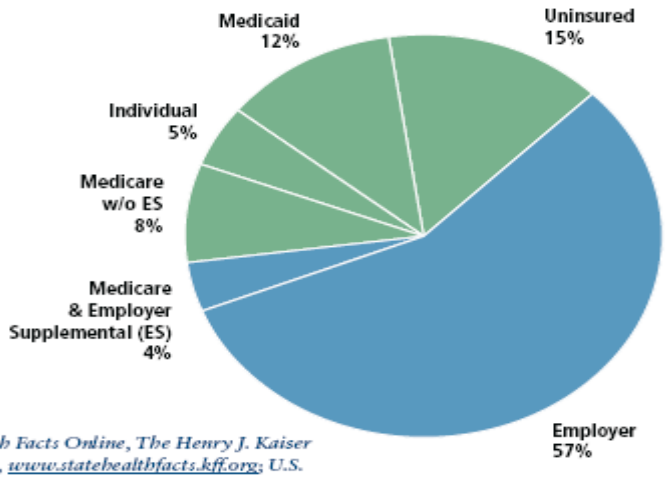
Table 1: Sample Data Elements for Commercial and Medicare Databases

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

THOMSON MEDSTAT

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.

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.

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.

PHRs: The bad and the ugly

Any PHR owned or controlled by:

- Insurers
- Employers
- Banks
- Credit card companies

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

EHRs: Designed for Data Mining

- Laws and ethics protecting medical records ***do*** apply to EHRs, but are being ignored as if HIPAA trumps state laws and medical ethics
- Security and privacy protections are inadequate
- *Financial model often is selling the data*
- Vendor contracts often give vendors ownership and/or rights to use and sell the data

Solutions: a Conceptual Framework

- Smart Consumers
- Smart Technology
- Smart Legislation

Smart consumers know their rights!

Only individuals can strike the “balance” between personal privacy and uses of PHI

– 2007 principles developed by the bipartisan Coalition for Patient Privacy spell out the rights consumers want in electronic health systems

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

www.patientprivacyrights.org

Smart Technology

- Smart Privacy
  - independent consent management tools control access to all PHI
  - independent health record trusts hold complete, lifetime PHI
- Smart Security
  - use of 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

New industry ‘best practices’ standards for privacy

- ***Enterprise agrees that consumers totally control access to PHI in HIT platforms or products***
- Enterprise agrees to adhere to the 2007 principles of Coalition for Patient Privacy and comply with future updates
- Enterprise undergoes independent third-party audits to prove compliance with privacy principles
- Enterprise allows no use of PHI without explicit informed consent

First implementation of ‘best practices’ standards for privacy: HealthVault

http://www.healthvault.com/

Meets ‘best practices’ standard for health IT industry – proves privacy works in the ‘real’ world

In addition:

- only email address required, no name/ID, can have pet accounts
- all platform application partners must meet same high privacy standards
- onsite advertisers may only use data for the purpose advertised
- safe searches inside platform (information brought inside, no tracking)

Technology corporations that signed the 2007 Coalition for Patient Privacy letter to Congress

(support the 2007 Privacy Principles)

http://www.patientprivacyrights.org/site/PageServer?pagename=Oct2007_Coalition_Press_Release

- Microsoft – HealthVault platform and applications
- Tolven – offers PHRs with multiple layers of encryption and PKI
- Universata
- Y-T-C – offers independent consent management tools that prevent disclosure without informed consent

Smart Legislation

Congress must restore privacy rights

- Restore the right to health privacy & make the 2007 Coalition for Patient Privacy's principles the law of the land

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

  (2006 Markey Privacy Amendment to HR 4157)

- Independent Health Record Trusts

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

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)

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

Restoring Privacy is Inevitable

- *Americans are waking up*. Patient Privacy Rights is just getting started:
  - Primary Focus: **The Public**
  - Congress
  - Media
  - Website
  - Campaign for Rx Privacy
  - Petitions, Letters, Alternative Forms

- Vendors that build **consumer control** of access to PHI into HIT products and systems will win in the marketplace

How You Can Help Restore Privacy

Add your voice to the thousands who have joined Patient Privacy Rights.

- Together we are far *more* powerful!

1) Sign up at: www.patientprivacyrights.org.

- Sign letters and petitions, get e-alerts, contact lawmakers

2) Ask providers to honor your rights to privacy.
Download privacy forms at:

- http://www.patientprivacyrights.org/site/PageServer?pagename=Right_To_Medical_Privacy_Statement&JServSessionIdr009=91n5w20hw1.app8b

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