Privacy: Essential for Quality Health Care

Presentation to NCVHS

Ad Hoc Workgroup for Secondary uses of Health Data

Perspectives on Uses of Health Data: Health Plan Perspectives

Deborah C. Peel, MD

Thursday August 2, 2007

patientprivacyrights

Key Points

- The common good, advancing the quality of health care in the nation, is *only* possible with privacy

- Transparency will not reassure individuals that their privacy is protected. Controlling all access to electronic health records, i.e. real consumer empowerment, is the only way individuals will be assured that their privacy is protected

- 'Smart technologies' that ensure consumer control of personal electronic health records are the only route to HIE and the only route to enable research uses of personal health information to improve health and the healthcare delivery system

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

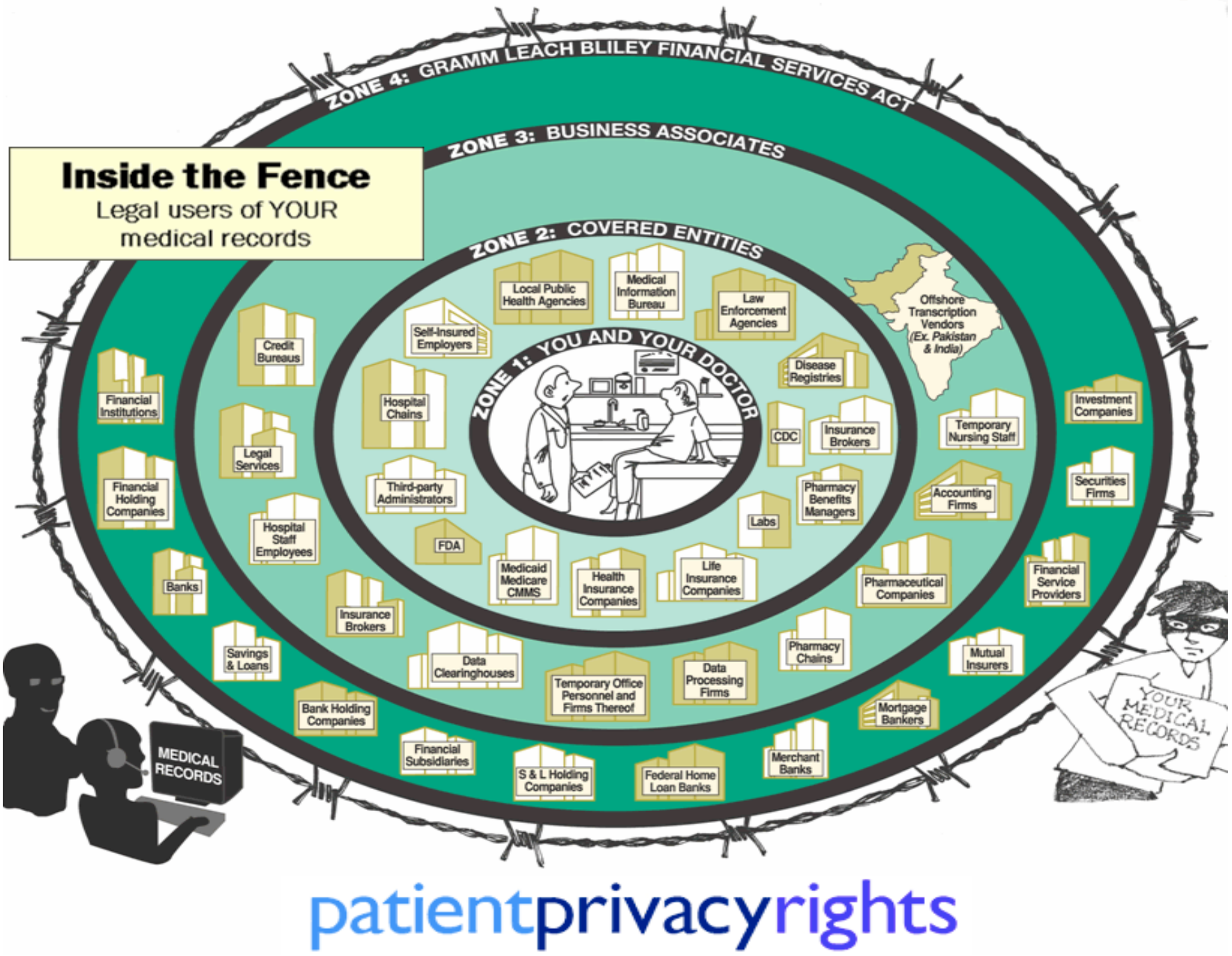
- Consumers don't know about the rampant secondary uses of their personal health information or how far outside the healthcare system their sensitive medical records flow
- HIPAA eliminated consent
- Coerced illegal consents (Rothstein article in JAMA)
- Data is worth billions to insurers, to employers, 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



patientprivacyrights

Effects of NO Health Privacy

- Denial of promotions/Job loss
  - 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 uninsurable and unemployable

patientprivacyrights

Privacy Rule is now a 'Disclosure Rule'

A Dose Of Bad Medicine:

"With an Orwellian turn of phrase, the ***'privacy rule' has little to do with patient confidentiality****. In fact, it permits the widespread sharing of medical data among 800,000 or so health, business and government entities."* The Philadelphia Inquirer, Editorial, 1/6/06

"The electronic information revolution is transforming the recording of health information so that disclosure of information may require only push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time." HHS at 65 Fed. Reg. at 82,465

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*
- *Paying privately for a test*
- *Asking a doctor to alter a diagnosis*
- *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

3/4 of the public want the government to set rules to protect the privacy and confidentiality of electronic health information.

2/3 want the government to set rules controlling the secondary uses of information.

Markle Foundation Survey, November 2006

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

UPI Poll: Concern on Health Privacy, February 21, 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

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

- for public health to detect disease outbreaks (73%)
- for 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

Law & Ethics

- Informational privacy is protected by the 4th, 5th and 14th Amendments to the United States Constitution. *
- *"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."* **
- All 50 states and the District of Columbia recognize in tort law a common law or statutory right to privacy of personal information. ***
- *"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).

*Whalen v. Roe, 97 S. Ct. 869, 877 (1977); Ferguson v. City of Charleston, 121 S. Ct. 1281, 1288 (2001)

**U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dodds, 419 F.3d 1097 (10th Cir. 2005).

***HHS finding 65 Fed. Reg. at 82,464

patientprivacyrights

Secondary Uses, Without Consent

- **Thomson Medstat sells data from Medicare, Medicaid, health plans, and the uninsured--** **WHITE PAPER** January 2006:**Health Research Data for the Real World: The MarketScan Databases, by** David M. Adamson, PhD, Stella Chang, MPH, Leigh G. Hansen, MS, MBA; Research and Pharmaceutical Division, Thomson Medstat

- **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

Unwanted/Unknown Secondary Users & Sellers

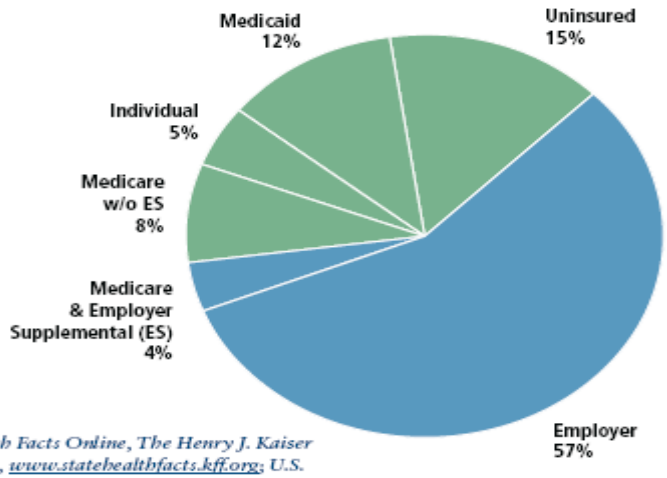
- Rx Switching companies, PBMs
- Technology Industry (via vendor contracts)
- Insurance Industry
- Data aggregators and data miners
- Hospital industry
- Transcription industry
- Banks and the financial industry (via GLB)
- Self-insured employers
- Quality Assurance/Improvement, hospital-based studies
- Research without consent (Privacy Act or IRB approved)
- State and Federal databases and registries
- Some Public health uses

patientprivacyrights

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.

patientprivacyrights

“Don’t Worry, We Won’t Look at That…”

FDIC Notice April 28, 2004 (excerpts)

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

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

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 Legislation

- *Congress must set national privacy policies*
- Federal right to health privacy & the 2007 Coalition for Patient Privacy's principles

  (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

Smart Technology

- Privacy
  - independent consent management tools control access to all PHI
  - independent health record trusts hold complete, lifetime PHI
- Security
  - state-of-the-art physical and technical standards
  - data encryption at rest and in transit
  - strong 2-factor authentication of users
  - PKI
  - firewalls
- 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

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

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