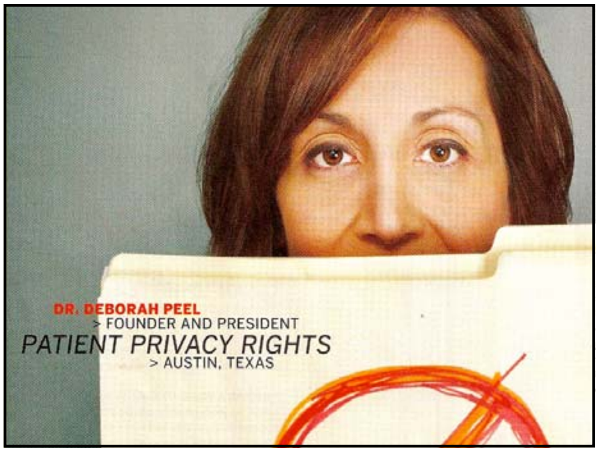
Views from the Top

WHY BOTHER WITH PRIVACY?

Tuesday, February 26, 2:15 PM - 3:15 PM

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

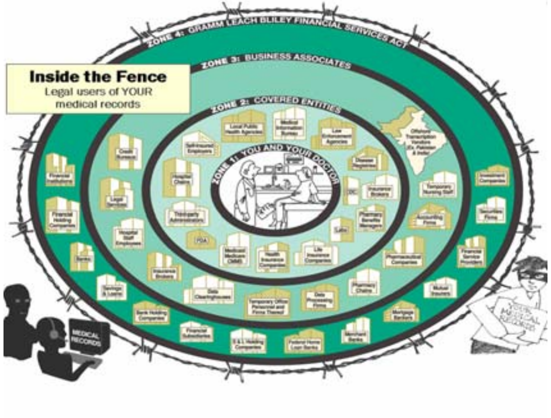
The elimination of consent

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."*

Congress intent was for HHS to recommend standards to protect the privacy of individually identifiable health information that included:

*(1) "**The rights that an individual** who is a subject of individually identifiable health information **should have"***

*(2) "**The procedures** that should be established **for the exercise of such rights."***



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.

"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."

Genetics & Public Policy CENTER

U.S. Public Opinion on Uses of Genetic Information and Genetic Discrimination

93% of the public does not think employers should access genetic test results

93% of the public does not think health insurers should access genetic test results

¾ of the public support laws to ban discrimination based on genetic tests

April 24, 2007

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.

United Healthcare's Ingenix unit now runs these massive virtual database operations, still in stealth-mode, for obvious reasons.

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.

Healthcare IT News

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** and by placing medically relevant ads within the EMRs, Howard said.*

*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.** Everyone has this data, but we'll have more of it and it will be real-time and aggregated," Howard said.*

"Based on our analysis of 30 PHR vendors, existing privacy policies are incomplete."

Review of the Personal Health Record (PHR) Service Provider Market, Privacy and Security, January 5, 2007

The report was developed for the Office of the National Coordinator for Health Information Technology (ONC) by Altarum Institute.

WorldVistA
www.worldvista.org

- Howard said the department's health care information system, known as VistA, has weaknesses since it was built at a time when the VA did not worry as much about security.
- The Veterans Affairs Department has set aside more than $20 million to respond to its latest data breach, the agency's top technology officer said Thursday.

VA sets aside $20 million to handle latest data breach, *Government Executive*, June 14, 2007

Personal health information is for sale

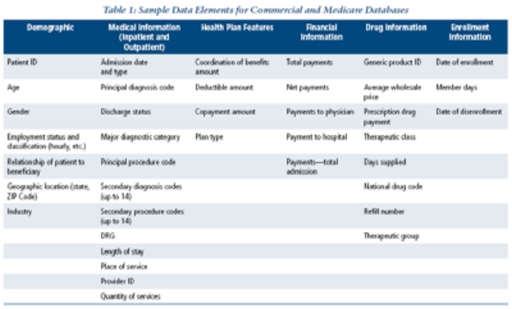
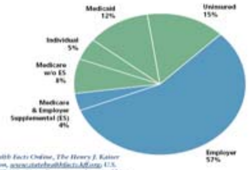


Table 1: Sample Data Elements for Commercial and Medicare Databases

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 – [illegible]. 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 insurers, with plans in all 50 states, announced the creation of a new business unit to aggregate and sell the claims and health records of all 79 million enrollees:

In a conversation with Patient Privacy Rights, 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."

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 the plan had been building the database, he had "never heard about privacy concerns."

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.

IOM Project Survey Findings on Health Research and 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.

"Today, the health industry relies upon the HIPAA construct of covered entities and business associates **to protect health data."**

"NCVHS proposes that all organizations and individuals with access to personal health data follow attributes of appropriate ***data stewardship*."**

"NCVHS recommendations describe the attributes of appropriate health data stewardship as including, but not limited to: accountability and chain of trust, transparency, individual participation, de-identification, security safeguards and controls, data quality and integrity, and oversight of data uses."

NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS December 19, 2007
Report to the Secretary of the U.S. Department of Health and Human Services On
Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data

"EHR-S provide a new opportunity for fraudulent behavior, and on ever-increasing scales…"

The more detailed information available to these pattern-detection systems, the greater the ability to differentiate legitimate from fraudulent behavior.

Detection of a fraudulent claim is often difficult when a payer has access only to EHR information for a single encounter. Reviewing information over an entire episode of care for a single patient allows greater ability to detect fraud.

Recommended Requirements for Enhancing Data Quality in Electronic Health Records
Final Report, May 2007 by RTI, Published by ONC June 2007

The Wall Street Journal

Spread of Records Stirs Patient Fears Of Privacy Erosion
Ms. Galvin's Insurer Studies Psychotherapist's Notes

By THEO FRANCIS

December 26, 2006; Page A1

After her fiancé died suddenly, Patricia Galvin left New York for San Francisco in 1996 and took a job as a tax lawyer for a large law firm. A few years later, she began confiding to a psychologist at Stanford Hospital & Clinics about her relationships with family, friends and co-workers.

Then, in 2001, she was rear-ended at a red light. When she later sought disability benefits for chronic back pain, her insurer turned her down, citing information contained in her psychologist's notes.

The notes, her insurer maintained, showed she wasn't too injured to work.

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

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)*

Is this what Americans want?

Newsfeed

Tom Jones wrote on ***Marisa Smith***'s wall:

"***Michael Thompson*** has herpes according to his latest prescription purchase at Rite Aid. Yikes!"

- Zuckerman: "It took us too long after people started contacting us to change the product…Instead of acting quickly, we took too long to decide on the right solution…People need to be able to **explicitly choose what they share, and they need to be able to turn Beacon off completely if they don't want to use it**."
- "In a way it kind of reminds me of an abusive husband who says, 'This is the last time I am going to act out.' It very rarely is," said Solove. "At the end of the day, the problem is that Facebook **thought [a] quick opt out will cure the problem. [Privacy] is about people having control over their information."**

Update: Facebook caves in to Beacon criticism.
Users skeptical the move will allay their privacy concerns; CEO admits 'mistakes'
ComputerWorld, December 5, 2007

Last year, AOL released the queries conducted by more than 650,000 Americans over three months to foster academic research.

While the queries where associated **only with a number**, rather than a computer's address, reporters for The New York Times and others were quickly able to identify some of the people who had done the queries.

The queries released by AOL included searches for deeply private things like "**depression and medical leave**" and "fear that spouse contemplating cheating."

Ask.Com Puts a Bet on Privacy, *New York Times*, Dec. 10, 2007

IP address is personal data: EU official

Last Updated: Tuesday, January 22, 2008 | 9:24 AM ET

The Associated Press

IP addresses, string of numbers that identify computers on the internet, should generally be regarded as personal information, the head of the European Union's group of data privacy regulators said Monday.

Germany's data protection commissioner, Peter Scharr, leads the EU group preparing a report on how well the privacy policies of internet search engines operated by Google Inc., Yahoo Inc., Microsoft Corp. and others comply with EU privacy law.

He told a European Parliament hearing on online data protection that *when someone is identified by an IP, or internet protocol, address "then it has to be regarded as personal data."*

Why Do the Right Thing?

Do it right now, avoid fixing it later:

"**Ask.com** is betting it will. The fourth largest search engine company will begin a service today called AskEraser, which allows users to make their searches more private."

Microsoft HealthVault:

Our Health Privacy Commitment

1. The Microsoft HealthVault record you create is controlled by you.
2. You decide what goes into your HealthVault record.
3. You decide who can see and use your information on a case-by-case basis.
4. We do not use your health information for commercial purposes unless we ask and you clearly tell us we may.

New industry 'best practices' standards for privacy

- ***Consumers totally control access to PHI in HIT platforms or products via informed consent***
- Enterprise agrees to adhere to the 2007 principles of Coalition for Patient Privacy and updates
- Independent third-party audits prove compliance with privacy principles

---

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

Smart Solutions

'Smart' Technology

- Health Trusts or Banks
- Independent Consent Management Tools

'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

NOT part of the Solution

Legislation without privacy

- Senate “Wired for Healthcare Quality Act” S 1693
  - “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)

Solutions

‘Smart’ 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.

Solutions

‘Smart’ Certification

PrivacyRightsCertified, Inc.

- Continually updates standards to address new and emerging threats to privacy, security, and confidentiality
- Assures legal compliance with the most stringent state, federal, and international privacy laws and rights.
- Governed by leading national consumer and privacy organizations and experts

patientprivacytoolkit

Forms
- Privacy Instructions: Give to all Providers
- How to Talk to Your Doctor
- For Physicians: Opt out of the AMA Database

Information
- Your Health Privacy Rights
- 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)

Forms
- Complaint Form to HHS
- Withdraw Consent -- *coming soon*

Information
- FAQs

Take Action
- 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 without strong privacy protections”
- Use the Consumer Tool Kit, ask providers to sign *your* privacy forms

www.patientprivacyrights.org

Will you Join Us?

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)

www.patientprivacyrights.org