Cambridge University

Electronic Health Records
Which is worse
the UK system or the US system?

Friday, September 5, 2008

Deborah C. Peel, MD

patientprivacyrights

Threats

US has no definition of ‘privacy’

What does ‘privacy’ mean?

Privacy means control over personal information.

Without control, you have no privacy.

Americans have no control over personal health data

HIPAA eliminated consent

1996 Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HHS) was required to develop regulations that specified patients' rights to health privacy.

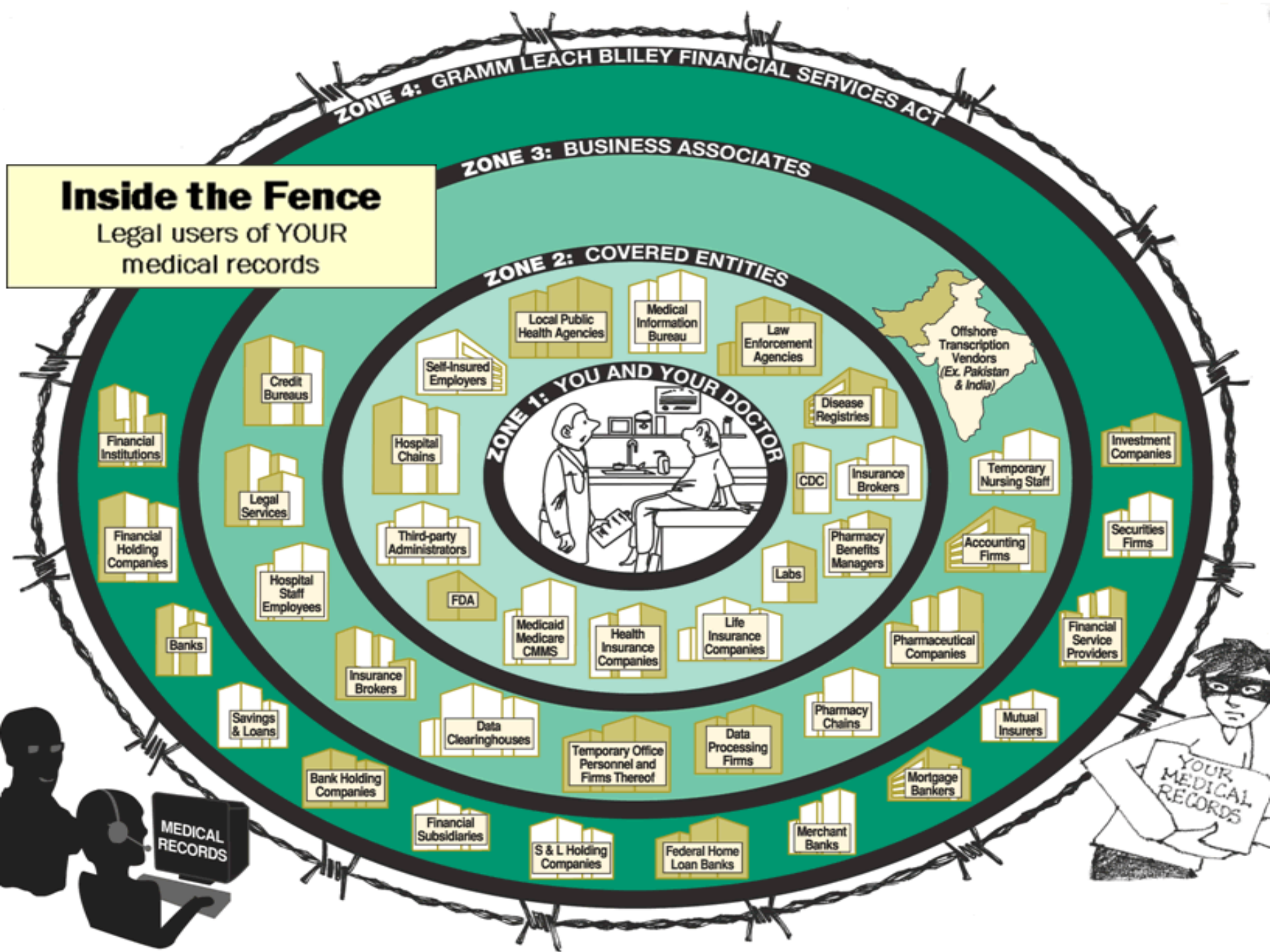
> *"… the Secretary of Health and Human Services shall submit to [Congress]…**detailed recommendations on standards with respect to the privacy of individually identifiable health information."***

2001 President Bush implemented the HHS HIPAA "Privacy Rule" which recognized the "right of consent".

> *"….a covered health care provider **must obtain the individual's consent,** in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations."*

2002 HHS amended the HIPAA "Privacy Rule", eliminating the "right of consent".

> *"The **consent provisions…are replaced** with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations."*


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

Consequences:

- **Job loss/ denial of promotions**
  - health data is used to discriminate
- **Data mining and sale of health data**
- Bad data/ no data = poor quality of research
  - people avoid participation, lie, omit
- Insurance discrimination

- *National Health IT system will fail*

American Employers Discriminate

- **35% of Fortune 500 companies admit to using medical records for hiring and promotions**

65 Fed. Reg. 82,467.

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

EHRs,PHRs, and prescriptions

Designed for Data Mining

- Weak Security
- No privacy
- Secondary Use

No trusted seal-of-approval for privacy and security (yet)

Weak Security

- Easy to hack
- Strong 2-factor authentication not required
- Data encryption at rest not required
- Loss/theft of mobile devices
- No role-based access, i.e., no consumer access controls (hacking from the inside)
  - In an 8-hospital system all 33,000 employees can access every patient record

Electronic medical records at risk of being hacked, report warns

CIO news

By Linda Tucci, Senior News Writer
19 Sep 2007 | SearchCIO.com

The electronic health record systems that automate the digitized medical histories of U.S. patients are severely at risk of being hacked, a new report has claimed.

"There was not one system we could not penetrate and gain control of data," said eHVRP board member Daniel S. Nutkis. "These systems were not any worse than banking systems. But the banking systems have elaborate security mechanisms sitting on top of them."

The eHVRP report is based on a 15-month study of more than 850 provider organizations.

NIH Data Breaches

- **Barton health records stolen and he's ticked**
  Dallas Morning News, April 3, 2008, by **Todd J. Gillman**
  Rep. Joe Barton revealed Thursday that he is one [of the 3,000+] heart patients whose medical records were on an unencrypted laptop stolen from a National Institutes of Health researcher.

- ***New York Times*** **Editorial re: NIH Breach,** March 26, 2008
  "There should be a federal law imposing strict privacy safeguards on all government and private entities handling medical data. Congress should pass a bill like the Trust Act, introduced by Representative Edward Markey, a Democrat of Massachusetts, imposing mandatory encryption requirements and deadlines for notifying patients when their privacy is breached. As the N.I.H. has shown, medical privacy is too important to be left up to the medical profession."

Georgia Patients' Records Exposed on Web for Weeks

The New York Times, April 11, 2008, by Brenda Goodman

- A company hired by the State of Georgia to administer health benefits for low-income patients is sending letters to notify tens of thousands of residents that their private records were exposed on the Internet for nearly seven weeks before the error was caught and corrected, a company spokeswoman said on Thursday.

- The records of as many as 71,000 adults and children enrolled in the Medicaid or PeachCare for Kids programs were inadvertently posted on Feb. 12, said Amy Knapp, a spokeswoman for the company, WellCare Health Plans Inc., whose headquarters are in Tampa, Fla.

COMPUTERWORLD

Portable Storage Devices Pose IT Security Risk

How much damage can a memory stick or iPod do? Plenty, say users and Analysts

March 27, 2006 (Computerworld) -- **Baptist Memorial Health Care Corp. in Memphis recently found itself dealing with a proliferation of user-owned plug-and-play USB port drives that posed a security risk to sensitive patient data**.

Lenny Goodman, IS director for desktop management at the health care company, said users found it difficult to copy significant amounts of data to floppy disks, and the company "did not allow CD writers."

So users turned to "the USB flash drive, with enormous capacity and zero installation," Goodman said earlier this month. "Very handy, very risky—both as a way for data to leave and a way for malware to arrive. We had to do something."

Recognizing the Risk

Eric Ouellet, an analyst at Gartner Inc. in Stamford, Conn., said that ***only about 10% of companies have any policies dealing with removable storage devices.***

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=management&articleId=109911&taxonomyId=14&intsrc=kc_feat

No privacy

- Over 4 million ‘covered entities’, including providers, self-insured employers, data warehouses, etc, can access protected health information for treatment, payment, and healthcare operations
- Millions more ‘business associates’ can use data without consent
- Audit trails NOT required for all uses and disclosures

Secondary Use

- The business model for many EHRs and PHRs is selling data for secondary use and data mining
- Major academic hospitals sell patient data
- Insurers sell data
- All prescriptions are data mined and sold

HealthcareITNews

Practice Fusion expands, shows signs of rapid growth

By Diana Manos, Senior Editor
12/31/07

Practice Fusion subsidizes its free EMRs by selling de-identified data to insurance groups, clinical researchers and pharmaceutical companies.

Howard said he does not expect data-sharing will be a concern to physicians who use Practice Fusion's EMRs. ***"Every healthcare vendor is selling data."***

EMR vendor sells patient data to for-profit genetics research firm

Healthcare IT News, 3/20/2008 by Richard Pizzi

- "Perlegen Sciences, Inc., a company exploring the clinical application of genetic research, plans to collaborate with an undisclosed electronic medical records vendor to identify and develop genetic markers that predict how patients are likely to respond to specific medical treatments.

- Under the terms of the agreement, Perlegen, based in Mountain View, Calif. , will have exclusive access to the EMR vendor's database of U.S. records for the purpose of assessing and selecting patients from whom appropriate genetic samples could be collected."

In August, 2006, a large insurer, with plans in all 50 states, announced the creation of a new business unit to aggregate and sell the claims and health records of 79 million enrollees:

The Medical Director said that the intended use of the database is to "service the big employers that pay the bills and want to pay smaller bills for health insurance."

He was "very enthralled about the ability to help multi-state employers fix their healthcare costs." During the one and one-half years that the plan had been building the database, he had "never heard about privacy concerns."

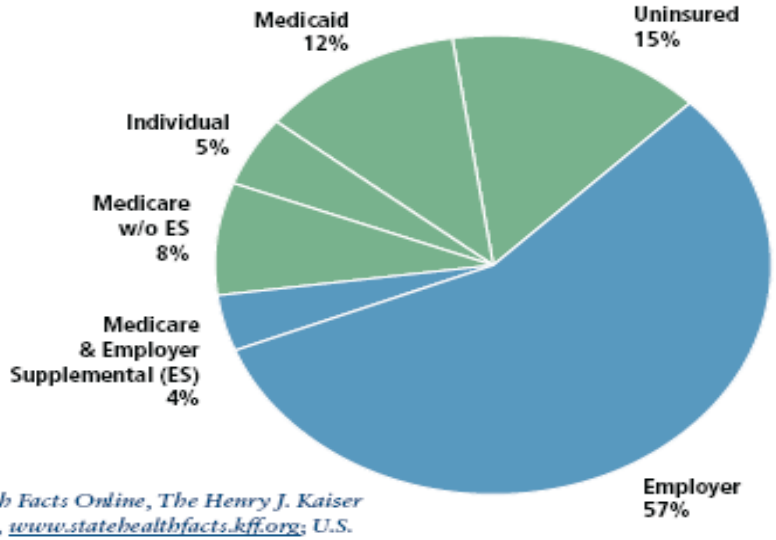
Personal health information is for sale

Table 1: Sample Data Elements for Commercial and Medicare Databases

Demographic	Medical Information (Inpatient and Outpatient)	Health Plan Features	Financial Information	Drug Information	Enrollment Information
Patient ID	Admission date and type	Coordination of benefits amount	Total payments	Generic product ID	Date of enrollment
Age	Principal diagnosis code	Deductible amount	Net payments	Average wholesale price	Member days
Gender	Discharge status	Copayment amount	Payments to physician	Prescription drug payment	Date of disenrollment
Employment status and classification (hourly, etc.)	Major diagnostic category	Plan type	Payment to hospital	Therapeutic class	
Relationship of patient to beneficiary	Principal procedure code		Payments—total admission	Days supplied	
Geographic location (state, ZIP Code)	Secondary diagnosis codes (up to 14)			National drug code	
Industry	Secondary procedure codes (up to 14)			Refill number	
	DRG			Therapeutic group	
	Length of stay				
	Place of service				
	Provider ID				
	Quantity of services				

Medicare and Medicaid data is for sale

Figure 1: Population Distribution by Insurance Status — 2002



Source: State Health Facts Online, The Henry J. Kaiser Family Foundation, www.statehealthfacts.kff.org; U.S. residents – 285,007,110. Note: Percentages do not add to 100% because of rounding.

To address the need for better data on privately insured Americans, Thomson Medstat created the MarketScan® data collection. Since its creation, MarketScan has been expanded to include data on Medicare and Medicaid populations as well, making it one of the largest collections of claims-based patient data in the nation. MarketScan data reflect the real world of treatment patterns and costs by tracking millions of patients as they travel through the healthcare system, offering detailed information about all aspects of care. Data from individual patients are integrated from all providers of care, maintaining all healthcare utilization and cost record connections at the patient level.

All 51,000 American pharmacies are data mined

- **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 acting as a powerful surrogate for the medical record itself.

- All of this is HIPAA compliant because the insurance company always has the release, signed by the individual applicant. United Healthcare's ***Ingenix unit now runs these massive virtual database operations, still in stealth-mode, for obvious reasons.***

Businessweek July 23, 2008:

"They Know What's in Your Medicine Cabinet, How insurance companies dig up applicants' prescriptions—and use them to deny coverage"

http://www.businessweek.com/magazine/content/08_31/b4094000643943.htm?chan=magazine+channel_in+depth

DATA ON DEMAND | Two companies dominate the field of selling prescription information to insurance companies:

	MEDPOINT	INTELLISCRIPT
Parent	UnitedHealth Group's Ingenix	Milliman
Location	Eden Prairie, Minn.	Brookfield, Wis.
History	UnitedHealth acquired MedPoint in 2002 from a small, Utah-based health-technology company, Nex2	Milliman, a Seattle consulting firm, acquired IntelRx and its IntelliScript product in 2005
Fine print	Delivers five-year history of drug purchases, dosages, refills, and possible medical conditions	Similarly provides five-year purchase history, which includes information on pharmacies and treating physicians
Pitch to insurers	"Identify high-risk individuals, reduce costs, lower loss ratios, and increase revenue"	"Clients report financial returns of 5:1, 10:1, even 20:1"

Data: MedPoint and IntelliScript


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

US Pharmacists Code of Ethics

1981

A Pharmacist *has the duty to observe the law, to uphold the dignity and honor of the profession, and to accept its ethical principles.*

A Pharmacist *should respect the confidential and personal nature of his professional records; except where the best interest of the patient requires or the law demands, he should not disclose such information to anyone without proper patient authorization.*

A Pharmacist *should not agree to practice under terms or conditions which tend to interfere with or impair the proper exercise of professional judgment and skill, which tend to cause a deterioration of the quality of his service, or which require him to consent to unethical conduct.*

1994

A pharmacist respects the covenantal relationship between the patient and pharmacist.

A pharmacist promotes the good of every patient in a caring, compassionate, and confidential manner.

A pharmacist serves individual, community and societal needs.

- However, the obligations of a pharmacist may at times extend beyond the individual to the community and society.

A pharmacist seeks Justice 'in the distribution of health resources.

- When health resources are allocated, a pharmacist is fair and equitable, balancing the needs of patients and society.

Royal Pharmaceutical Society of Great Britain

3. SHOW RESPECT FOR OTHERS

Demonstrating respect for the dignity, views and rights of others is fundamental in forming and maintaining professionally appropriate relationships with patients, their carers, colleagues and other individuals with whom you come into contact with. In your Professional practice you must:

3.5 Respect and protect the dignity and privacy of others. Take all reasonable steps to prevent accidental disclosure or unauthorised access to confidential information and ensure that you do not disclose confidential information without consent, apart from where permitted to do so by the law or in exceptional circumstances.

3.6 Obtain consent for the professional services, treatment or care you provide and the patient information you use.

3.7 Use information obtained in the course of professional practice only for the purposes for which it was given or where otherwise lawful.

6. BE HONEST AND TRUSTWORTHY

Patients, colleagues and the public at large place their trust in you as a pharmacy professional. You must behave in a way that justifies this trust and maintains the reputation of your profession. You must:

6.3 Avoid conflicts of interest and declare any personal or professional interests to those who may be affected. Do not ask for or accept gifts, inducements, hospitality or referrals that may affect, or be perceived to affect, your professional judgement.

6.6 Comply with legal requirements, mandatory professional standards and accepted best practice guidance.

IOM Survey: People Won't Participate in Research Without Privacy

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

- Only 1% agreed that researchers would be free to use personal medical and health information without consent
- Only 19% agreed that personal medical and health information could be used as long as the study "never revealed my personal identity" and it was supervised by an Institutional Review Board.

“It’s pretty clear that the public is afraid of taking advantage of genetic testing,” said Dr. Francis S. Collins, director of the National Human Genome Research Institute at the National Institutes of Health.

“If that continues, the future of medicine that we would all like to see happen stands the chance of being dead on arrival.”

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.

Opportunities

Smart Solutions

‘Smart’ Legislation

‘Smart’ Technology

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

‘Smart’ Certification

‘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

Trusted Certification

PrivacyRightsCertified, Inc.

Consumer-led organization offering a Good Housekeeping Privacy Seal-of-Approval for HIT systems and products that ensure consumer control of PHI

Privacy Rights Certified will ensure Americans **UNDERSTAND** PHRs and EHRs, **CHOOSE** wisely, and take steps to **PROTECT** their most intimate information.

Privacy certification program aims to ensure patients' trust

www.digitalhcp.com/2008/09/03privacy.html

HHS adviser and privacy advocate tackle health IT privacy

www.ihealthbeat.org/articles/9/4/Former-HHS-Adviser-Privacy-Advocate-Tackle-Health-IT-Privacy.aspx?topicID=54

Progress with Privacy:
Join Patient Privacy Rights

www.patientprivacyrights.org

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

Ashley Katz, MSW
Executive Director
akatz@patientprivacyrights.org

512.732.0033 (office)