OPEN MINDS
Technology and Informatics Institute

Have we seen the end of consumer privacy in health care?

October 17, 2012

Deborah C. Peel, MD

patientprivacyrights

why consent and control are needed:

the surveillance economy

government fusion centers

corporate data mining industry

The New York Times

Not Track? Advertisers Say ‘Don’t Tread on Us’

By NATASHA SINGER
October 13, 2012 http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html?_r=1&ref=natashasinger

--campaign to defang the “Do Not Track” movement began late last month

--“what is really at stake here is the future of the surveillance economy”

--House to FTC: ‘Do Not Track’ might restrict “the flow of data at the heart of the Internet’s success.”

-- open letter from the board of the Association of National Advertisers: Microsoft’s action is wrong. The entire media ecosystem has condemned this action”

The New York Times

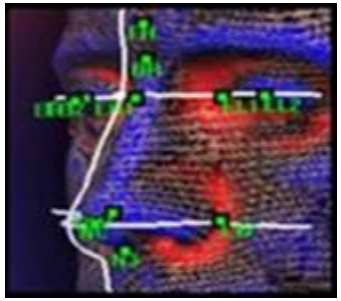
How Companies Learn Your Secrets

By Charles Duhigg
Published: February 16, 2012

“If we wanted to figure out if a customer is pregnant even if she didn’t want us to know, can you do that? ”

http://www.nytimes.com/2012/02/19/magazine/shoppinghabits.html?pagewanted=all

BEYOND FINGERPRINTS FUSION CENTERS



Biometric Databases and Quantitative Privacy

by Danielle Citron September 8, 2012

$1B next generation ID system

multimodal biometrics: palm prints, fingerprints, iris, retina, voice, face, gait

Data from state, local, & federal law enforcement; mug shots, DNA databases, driver ID photographs; **federal, state, & local fusion centers mine information** posted online, private security camera footage, & systems of private partners.

http://www.concurringopinions.com/archives/2012/09/biometric-databases-and-quantitative-privacy.html#more-65882

You for Sale: Mapping, and Sharing, the Consumer Genome

June 16, 2012
Justin Bolle for the New York Times

Acxiom--world's largest consumer database

- 50 trillion data transactions/year.
- 500M consumers worldwide, a majority of US adults
- **sales of $1.13B**
- **1,500 data points per person**

http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database marketing.html?_r=3&ref=todayspaper

The Wall Street Journal

Insurers Test Data Profiles to Identify Risky Clients

By Leslie Scism and Mark Maremont

NOVEMBER 19, 2010

Life insurers are testing an intensely personal new use for the vast dossiers of data being amassed about Americans: predicting people's longevity.

Data-gathering companies have such extensive files on most U.S. consumers—online shopping details, catalog purchases, magazine subscriptions, leisure activities and information from social-networking sites—that some insurers are exploring whether data can reveal nearly as much about a person as a lab analysis of their bodily fluids.

http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html

Can Marketing Data Predict Life Spans?

Deloitte Consulting uses a hypothetical 'Sarah' and 'Beth' to promote technology for life insurers that promises to help size up people's health risk using offline and online dossiers rather than blood tests.

SARAH

Some data collected

SECOND CHILD BORN LAST YEAR
HIGH INVESTMENT RISK TOLERANCE
LIVED IN HOME – TWO YEARS
OWNS HOME
COMMUTING DISTANCE – ONE MILE
READS DESIGN AND TRAVEL MAGAZINES
URBAN SINGLE CLUSTER
PREMIUM BANK CARD
GOOD FINANCIAL INDICATORS
ACTIVE LIFESTYLE: RUN, BIKE, TENNIS, AEROBICS
HEALTHY FOOD CHOICES
LITTLE TO NO TELEVISION CONSUMPTION

BETH

CURRENT RESIDENCE – FOUR YEARS
LIVED IN SAME HOMETOWN – 15 YEARS
CURRENTLY RENTING
COMMUTING DISTANCE – 45 MILES
WORKS AS ADMINISTRATIVE ASSISTANT
DIVORCED WITH NO CHILDREN
FORECLOSURE/BANKRUPTCY INDICATORS
AVID BOOK READER
FAST-FOOD PURCHASER
PURCHASES DIET, WEIGHT LOSS EQUIPMENT
WALKS FOR HEALTH
HIGH TELEVISION CONSUMPTION
LOW REGIONAL ECONOMIC GROWTH

Some risk-assessment factors

- Good financial indicators
- Strong ties to community/location
- High activity indicators
- Foreign traveler
- Healthy food choices
- Avid outdoor enthusiast
- Avid golfer
- Little television consumption
- Occasional tobacco user
- Average commute
- Poor financial indicators
- Purchases tied to obesity
- High television consumption
- Lack of exercise
- Long commute

Potential actions by insurers

SARAH

Actively pursue for new business and retention efforts

Quickly issue a preferred policy and avoid further medical tests

BETH

Do not send offers

Do not pursue aggressive retention efforts

Collect more information; send to senior staffer for review

Source: Deloitte Consulting

Behavioral Advertising

http://www.aboutads.info/choices/

113 companies participate in the self-regulatory program

Using the tools on this page, you can opt out from receiving interest-based advertising from some or all of our participating companies:

24/7 Media	Adara Media, Inc.	etc
33Across	Adblade Premium Ad Network	etc
Accuen Inc.	AdBrite, Inc.	
Acxiom	Adchemy, Inc.	
Adap.tv, Inc.	Adconion Media Group	

myths about health privacy

- HIPAA protects privacy
- de-identified data is safe
- patients must give up privacy to benefit from HIT

HIPAA regs eliminated consent and privacy

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. **Public Law 104-191**

*"… 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 HIPAA "Privacy Rule" which recognized the "right of consent". HHS wrote these regulations.
65 Fed. Reg. 82,462

*"….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.
67 Fed. Reg. 53,183

*"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."*

Referred Doctors

Family members

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

Local Public Health Agencies
Medical Information Bureau
Law Enforcement Agencies
Offshore Transcription Vendors (Ex. Pakistan & India)
Self-Insured Employers
Credit Bureaus
Disease Registries
Financial Institutions
Hospital Chains
Investment Companies
Legal Services
CDC
Insurance Brokers
Temporary Nursing Staff
Financial Holding Companies
Third-party Administrators
Pharmacy Benefits Managers
Securities Firms
Hospital Staff Employees
Labs
Accounting Firms
FDA
Banks
Medicaid Medicare CMMS
Health Insurance Companies
Life Insurance Companies
Pharmaceutical Companies
Financial Service Providers
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
Merchant Banks
S & L Holding Companies
Federal Home Loan Banks

www.patientprivacyrights.org

HIPAA loopholes allow sale of data from EHRs, PHRs, claims data, lab data, prescriptions, health searches, state data, newborn bloodspots, etc, etc

big market for health data,
gaps in law, no enforcement,
theft and sale of health data,

health data mining industry

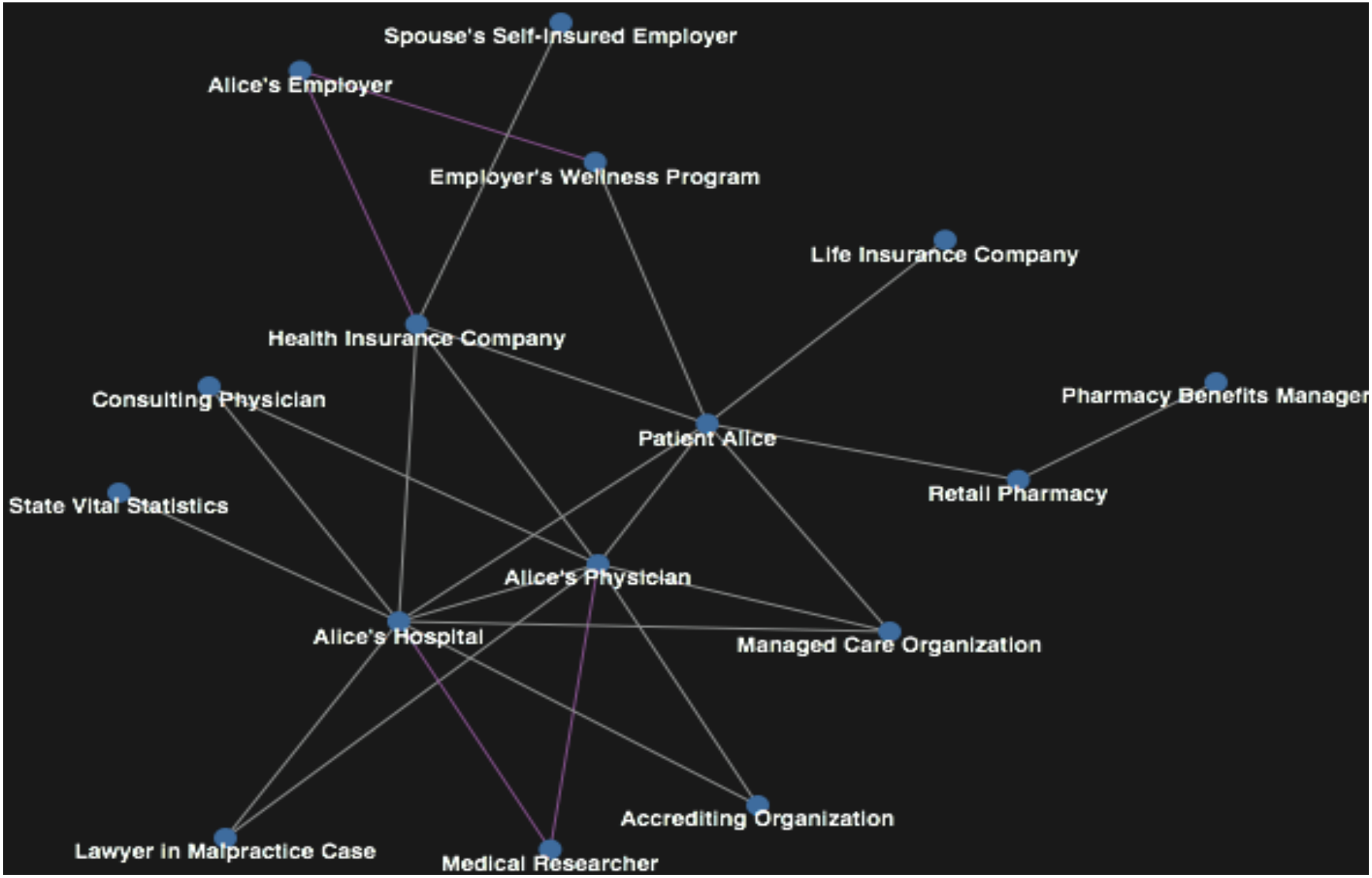
Prof. Latanya Sweeney

Secondary use of PHI by BAs is "unbounded, widespread, hidden, and difficult to trace."

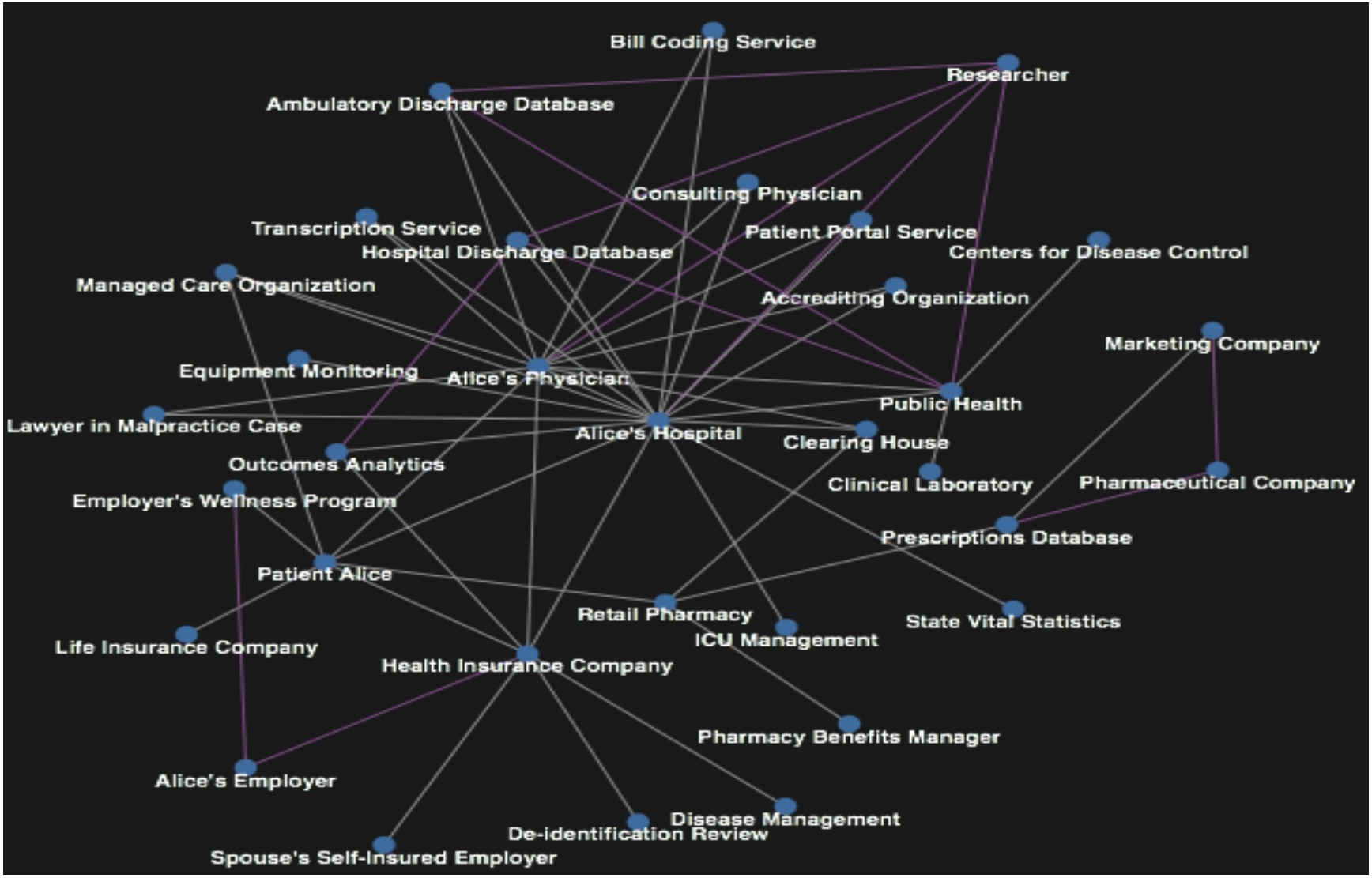
Implementing 'meaningful use' **EHRs will "increase data sharing, but adding the NHIN will massively increase data sharing**."

Proposed NwHIN models to link all Americans' health information online **do not offer "utility or privacy".**

http://patientprivacyrights.org/wp-content/uploads/2010/04/Sweeney-CongressTestimony-4-22-10.pdf



US Health data map 1997 http://tiny.cc/thxtlw



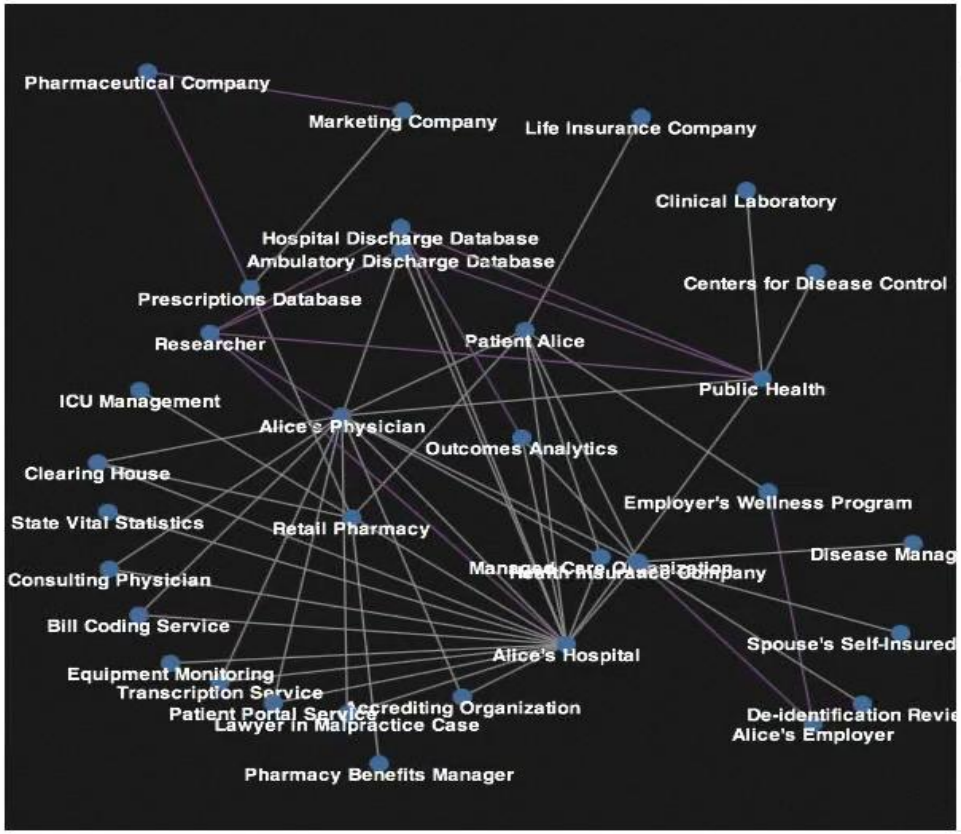
US Health data map 2010 http://tiny.cc/thxtlw

theDataMap™

Maps Highlights Features
News About
Login Sign-up Rankings
Contact Sponsors

theDataMap™ is under development. Sign-up for updates.

The crowd-updated and verified map of personal data flows will be here, publicly available, changing over time to show the current state of knowledge. Below is the initial map, pre-launch. (More about the project...)



Public Health

Connections:

- Alice's Physician
- Alice's Hospital
- Ambulatory Discharge Database
- Clinical Laboratory
- Hospital Discharge Database
- Researcher
- Centers for Disease Control

Reload page for a different configuration. **Drag** nodes around to reposition. **Scroll** to zoom and pan.
Click on a node to display details in right column.

PLEASE----Donate to PPR o help build theDataMap.org

HITECH:
$27B & historic new consumer protections for health IT and data exchange

BUT….government & HIT systems ignore privacy rights in:

- federal and state law
- common law
- tort law
- US Supreme Court decisions re: rights to health information privacy

existing privacy rights *NOT* built into EHRs or data exchanges:

- authorization is required to disclose "psychotherapy notes"
- technology to disclose only "minimum necessary" data
- consent is required before sale of PHI
- data cannot be disclosed to insurer if patient pays
- right to segment sensitive data (mental health, DNA, STDs)

- consent is required to disclose addiction treatment records (42 CFR Part 2)
- consent is required to disclose PHI outside military health system (USC 7332, Title 38, Veteran's Benefits)
- audit trail of disclosures of PHI x 3 years
- encryption---industry compliance abysmal <20%
- consent technologies---2014 or later
  (first test 2012)

the future

patient-controlled health IT systems & data exchanges

Don Berwick: “Medical records would belong to patients. Clinicians, rather than patients, would need to have permission to gain access to them.”

tech solutions

steps to patient-controlled health system:

- patient and physician portals
- strong ID: OAuth, OpenIDConnect, User Managed Access (UMA), UProve
- Direct Project--secure email exchange
- Blue Button---patients download electronic copies of data

tech solutions

- RHEx–patient tokens allow physicians to view select data
- metadata tagging to provide privacy
- independent consent management systems (data holders electronically check patient's preferences)
- health data banks

legal/policy solutions

- restore federal right of consent
- define ‘privacy’
- trust framework based on FIPS
- ‘chain of custody’ for data
- ‘veto’ - only PHI for treatment
- ‘privacy impact assessments’

summary

- we are immersed in a surveillance economy
- we still have very strong rights to protect PHI
- we must move from organizational to personal control over PHI

If we LOSE the right to control PHI, will we ever gain control over any other personal information in the Digital Age?

Will you help? PLEASE donate to build the DataMap:

www.patientprivacyrights.org

Deborah C. Peel, MD

Founder and Chair

(O) 512-732-0033

dpeelmd@patientprivacyrights.org

www.patientprivacyrights.org

patientprivacyrights