Health Data Privacy

Ben Adida
Children’s Hospital Informatics Program
Center for Research on Computation and Society

16 October 2008
HST950

“Let’s put health records online!”

John McCain
October 7th 2008

Privacy is Important

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence

[...]
Everyone has the right to the protection of the law against such interference.

Article 12, Universal Declaration of Human Rights, United Nations.
Privacy is Dead

“Privacy is dead, deal with it,”
Scott McNealy (Dec. 2000)

People Don’t Care About Privacy

Passwords revealed by sweet deal
More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.

Morpace Reports: Electronic Medical Records Viewed Favorably, but Many Have Privacy Concerns

Morpace Omnibus study, fielded in September, reveals that 48 percent of American adults support creation of a nationwide system of medical records, while 23 percent oppose such a system.

More notably, however, survey participants cite significant privacy concerns about a national medical record system. Fear of identity theft tops the list, along with unauthorized access to an individual’s medical information by marketing firms, employers and even health insurance companies.

94043
Male
11/29/1976

87% of the population is uniquely identified
[Sweeney, CMU, 2000-2001]
ACGCTTAATCTAGGAGTATG

20 randomly selected SNPs in a genome record form a unique identifier

Good health care requires access to data

COX-2 selective inhibitors are associated with myocardial infarction (MI). We sought to determine whether population health monitoring would have revealed the effect of COX-2 inhibitors on population-level patterns of MI. METHODOLOGY/PRINCIPAL FINDINGS: We conducted a retrospective study of inpatients at two Boston hospitals, from January 1997 to March 2006. There was a population-level rise in the rate of MI that reached 52.0 MI-related hospitalizations per 100,000 (a two standard deviation exceedence) in January of 2000, eight months after the introduction of rofecoxib and one year after celecoxib. The exceedence vanished within one month of the withdrawal of rofecoxib.

HIPAA is not about Privacy

“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, and health care operations.” 67 Fed. Reg.
HIPAA complicates patient care

“In this national survey of clinical scientists, only a quarter perceived that the rule has enhanced participants’ confidentiality and privacy, whereas the HIPAA Privacy Rule was perceived to have a substantial, negative influence on the conduct of human subjects health research, often adding uncertainty, cost, and delay.”

http://jama.ama-assn.org.ezpl.harvard.edu/cgi/content/full/298/18/2164
http://www.msnbc.msn.com/id/21774591/

HIPAA Privacy Rule

- protects identifiable personal health info (must be a HIPAA covered entity.)
- does not protect “de-identified” data.
- made to ease the transfer of data between covered entities.

Established CHIP Projects
The Indivo PCHR

- A copy of the record that belongs to the patient
- The patient *controls* the record and its sharing
- Aggregation over the patient's lifetime
- Empower the Patient

Basic Security Features

- Application-level encryption
- Startup key unlock
- Encrypted swap partition
- Standards-based access control and logging.
• Non-profit consortium


• Built on Indivo

• Beta Launch happening now
**Control:** Dossia gives you control over your health information. Except when legal obligations or uncommon technical issues arise, you control to what degree and with whom to share it. In particular, and **without exception, your employer does not have access to your health information,** your Dossia usage patterns, or even the fact that you have chosen to use Dossia.

**Gene Partnership Project**

- HIPAA hurts research and patients
- Can we **reconnect** doctors and patients with
  - an improved consent process
  - better technology

---

**CHIP Projects in Development**
PCHR as a Platform

- “The Facebook Platform for Health Data”
- Privacy/Consent Management
- An ecosystem of innovation with a strong privacy foundation.

Building a Privacy-Protecting Platform
While Facebook may hold data hostage, all PCHR believe in data portability.

The fallacy of “the user clicked OK.”

Maybe we need a bit of paternalism.

Before we can warn you about serious diseases that may affect you, please agree to the privacy policy:

[...]
**Auth Setup**

1. User's Browser
2. Indivo Server
3. Access Token
4. PHA
5. Access Token
6. Indivo Server

**PHA in Action**

1. User's Browser
2. Indivo Server
3. Access Token
4. PHA
5. Access Token
6. Indivo Server
OAuth Actors

User's Browser

Indivo Server

PHA

OAuth Actors

Indivo Server (Data Service)

signed
HTTP+POX

PH (Consumer)

User's Browser

connection
Step (1)

GET request_token

add

token

REDIRECT authorize

Connection Step (2)

REDIRECT authorize

Authorization Process

post-add
OAuth Request

Authorization: OAuth realm="https://api.mydossia.org/",
    oauth_consumer_key="0685bd9184jfhq22",
    oauth_signature_method="HMAC-SHA1",
    oauth_signature="wOJI09A2W5mFw0giDvZb7SMK%2FPY%3D",
    oauth_timestamp="137131200",
    oauth_nonce="4572616e48616d657261686176",
    oauth_version="1.0"

Extensions

- Stronger authentication of PHAs
- Data Use Intent
  what will the PHA use the data for?
- Pingback Auditing
  letting the PCHR know data spread
- Sandboxed Applications?
Data-Use Intent

- **Access Pattern**
  - none, on patient demand, update-driven, omnipotent

- **Storage of Individual Data**
  - none, encrypted, unencrypted

- **Use of Individual Data**
  - none, for user, for redistribution/resale

- **Use of Aggregate Data**
  - none, for users, for redistribution/resale

Privacy Icons

In Summary

- Patient Control via **informed** consent
- disclosure, pingback, sandboxing.
- A platform that attempts to balance **innovation** and **user privacy**.