

# World Privacy Forum

***Lost in Translation: Consumers' risk-benefit perspectives on electronically mediated health care initiatives, services, and related issues***

FTC Health Care Innovations Workshop

April 24, 2008

Pam Dixon, executive director

- *Where* is the Archimedean point in this area?
- *What* does that supra-view look like?

# **View One: Medical Identity Theft**

## Medical identity theft is.....

“Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity – such as insurance information -- without the person’s knowledge or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name.” *World Privacy Forum, May 2006*

## Core Harms of Medical Identity Theft

Medical identity theft can wreak havoc on victim's lives:

- changes to the medical file
- changes to insurance billing codes
- insurance caps reached
- changes to credit report (collections)
- changes to insurance rates
- problems with employment, insurance, even law enforcement

## Where is the risk?

...Wherever there is data flowing in the health care sector's *Trust Architecture*. [\*]

- Institutional providers
- Profound risk in some electronic health exchanges
- **National Health Information Network (NHIN) pilots** - no risk assessments or mitigations for medical identity theft
- EHRs: some systems, esp. those not yet flexible enough to allow red-flagging for fraud

\* See World Privacy Forum testimony before AHIC on the Trust Architecture and its implications in the digital environment, <<http://www.dhhs.gov/healthit/ahic/materials/meeting09/cps/P2-PHR-Dixon.pdf>>

- ***Operationally, Insider Access*** is the most significant threat
- Clinic Takeover
- “One-off”

...Just one example, simply the most recent as of April 2008.... New York Presbyterian Hospital: a patient admission representative accessed **49,841 patient records** through the patient registration system, and sold thousands of the records to people he knew were going to commit crimes using the information, including identity theft and fraud.

## **View Two: Personal Health Records (PHRs)**



Medical Privacy	PHR Privacy
Hippocratic Oath, 4th century b.c.	Commercial PHR vendors have primary responsibility to shareholders/investors
Codes of medical ethics; 1800s: Percival's Code, 1847: AMA, others.	PHR vendor disclaims liability for patients
Physician-patient privilege (in many states) dating from 1828	PHR vendor excludes remedy for patients in privacy policy/TOS
Record keeper tort and malpractice liability for confidentiality violations	PHR privacy policy/TOS require patient to indemnify the PHR vendor
<b>Legal Confidentiality Standards:</b> <ul style="list-style-type: none"> <li>•Federal Alcohol and Drug abuse confidentiality Rules</li> <li>•State genetics and HIV/AIDs laws (most states)</li> <li>•HIPAA</li> </ul>	Privacy policy subject to change by PHR vendor at any time

\* PHR privacy column partially based on Revolution Health privacy policy, last viewed April 12, 2008, clauses 20-23. PHR privacy levels will differ based on each company's privacy policy.

**View Three: Consumer-Initiated Genetic Tests and Direct-to-Consumer Marketing of Genetic Tests (...one example among many possible examples)**

## Core Harms:

- Data leakage and subsequent secondary use
- Potential for long-lasting impact (sometimes for the duration of a life span) on victim and potentially blood relatives (employability, insurability)

## •Where is the risk?

- ...risk separates into several distinct areas, one risk area is the quality and utility of the test itself; another risk area is how the information about the patient is handled, and another is how the genetic data is handled.

- Certain kinds of online ads can pose potential consumer issues, particularly in combination with other online profiling. Even a request for a genetic test can potentially become lucrative information for marketing or for sale.

- Privacy policies may either not exist or they can be incomprehensible to consumers. GWAS research, ex.

- Will bad actors selling snake oil tests tarnish legitimate genomic innovations?

- Resources:

- *Medical ID Theft: The Information Crime that Can Kill You* [ report ] The medical identity theft report and FAQ for victims, plus 8 best practices for providers are located at the Medical ID theft landing page:  
<http://www.worldprivacyforum.org/medicalidentitytheft.html>
- *Why Many PHRs Threaten Your Privacy* [report and consumer advisory ]  
[http://www.worldprivacyforum.org/personal\\_health\\_records.html](http://www.worldprivacyforum.org/personal_health_records.html)
- *Electronic Health Records and the National Health Information Network: Patient Choice, Privacy, and Security in Digitized Environments*. Testimony before the National Committee on Vital and Health Statistics (NCVHS)  
<http://www.ncvhs.hhs.gov/050816p2.html>
- American Health Information Community (AHIC) testimony on electronic trust architectures and patient identity proofing:  
<http://www.dhhs.gov/healthit/ahic/materials/meeting09/cps/P2-PHR-Dixon.pdf>