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?

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 2007.6 Tm(“One-off”)TjEMC /P <</MCID 6 >>BDC -0.0006 Tc 0.0

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
Legal Confidentiality Standards: •Federal Alcohol and Drug abuse confidentiality Rules •State genetics and HIV/AIDs laws (most states) •HIPAA	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)

- 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

- *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