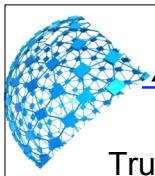


Trustworthy Designs for the Nationwide Health Information Network

Latanya Sweeney, PhD
Harvard, MIT, Carnegie Mellon

latanya@seas.harvard.edu AdvanceHIT.org

1

Thanks to Lillie Coney and

- Center for Financial Privacy and Human Rights
- Consumer Action
- Electronic Frontier Foundation
- Electronic Privacy Information Center
- Fairfax County Privacy Council
- Liberty Coalition
- National Center for Transgender Equality
- National Network to End Domestic Violence
- National Workrights Institute
- Patient Privacy Rights
- Privacy Rights Clearinghouse
- Privacy Times
- U.S. Bill of Rights Foundation
- U.S. Public Interest Research Group

2

Disclaimer

The views and opinions in this presentation represent my own and are not necessarily those of HHS, ONC or the Obama Administration. These views are for the benefit of public discourse and public education, and are not necessarily an opinion regarding any position I may take on related issues decided by the HIT Policy Committee.

3

Team Members

Harvard
- Stephen Chong, PhD
- Margo Seltzer, PhD
- Latanya Sweeney, PhD
- Salil Vadhan, PhD
- Jim Waldo, PhD

MIT
- Hal Abelson, PhD
- Tim Berners-Lee, PhD
- Lalana Kagal, PhD
- Gerald Sussman, PhD
- Peter Szolovits, PhD

WPI
- Isa Bar-On, PhD
- Sharon Johnson
- Renata Konrad, PhD
- Diane Strong, PhD
- Bengisu Tulu, PhD

4

Given the power of technology design and the stimulus thrust to build the nationwide health information network (NHIN),

Explore trust issues in NHIN designs.

Sweeney, L. *Towards Trust in the Nationwide Health Information Network.* Advance HIT Project. White Paper 1005. Harvard University. 2010.
In progress and under advisement! (latanya@seas.harvard.edu AdvanceHIT.org)

5

Given the power of technology design and the stimulus thrust to build the nationwide health information network (NHIN),

Explore trust issues in NHIN designs.

6

Ways to Effect Change

Law

Market forces

Social norms

Technology Design Code for architecture

Lawrence Lessig. *Codev2*. http://codev2.cc/.
Earlier version: *Code and Other Laws of Cyberspace*

7

Law

Technology Design

Sweeney re-identification of children in cancer registry using publicly available online data (1999). Court sealed process. [Southern Illinoisan v. Dept. of Public Health].

8

Market forces

Technology Design

iPod. Not the first MP3 player, but its seamless network design for purchasing and loading music transformed the market.

9

Social norms

Technology Design

Mobile phone and email; Facebook.
Growing expectation that people (and information about people) are immediately accessible.

10

Carnegie Mellon
DATA PRIVACY LAB

Privacy Technology

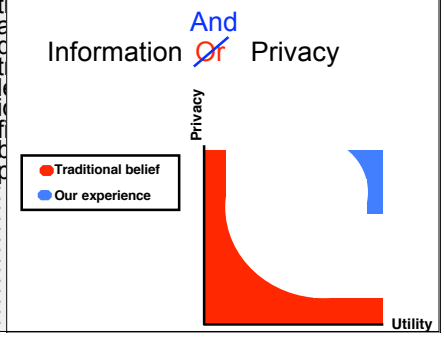
1. Example: tracking people
2. Example: anonymizing data
3. Example: distributed surveillance
4. Example: trails of dots
5. Example: learning who you know
6. Example: identity theft
7. Example: fingerprint capture
8. Example: bio-terrorism surveillance
9. Example: privacy-preserving surveillance
10. Example: DNA privacy
11. Example: SSN failures and biometrics
12. Example: k-Anonymity
13. Example: webcam surveillance
14. Example: text de-identification
15. Example: face de-identification
16. Example: fraudulent Spam

privacy.cs.cmu.edu

Carnegie Mellon
DATA PRIVACY LAB

Privacy Technology

1. Example: t
2. Example: a
3. Example: d
4. Example: t
5. Example: l
6. Example: i
7. Example: f
8. Example: b
9. Example: p
10. Example:
11. Example:
12. Example:
13. Example:
14. Example:
15. Example:
16. Example:



Given the power of technology design and the stimulus thrust to build the nationwide health information network (NHIN),

Explore trust issues in NHIN designs.

13

Nationwide Health Information Network (NHIN)

Vision is to share health data widely.

Evidence exists that doing so can offer significant improvements to patient care and dramatic reductions in costs.

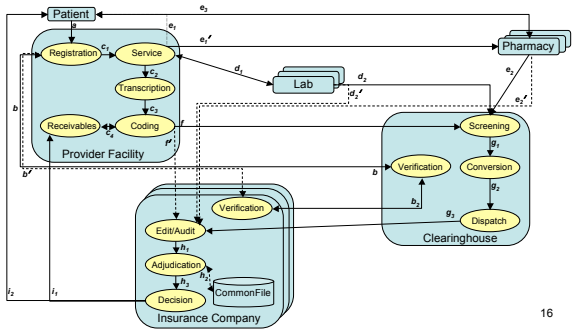
Chaudhry et al., Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care. *Annals of Internal Medicine*, Vol. 144, No. 10, 2006.

Health Data

Claims	Clinical
Sharing: insurers & others not include clinical data.	Sharing: providers & others not include all local data.
Optimized for income.	Documents patient care.
National connectivity processing billions of claims a year.	Few, disparate local areas processing select data from some patient visits.

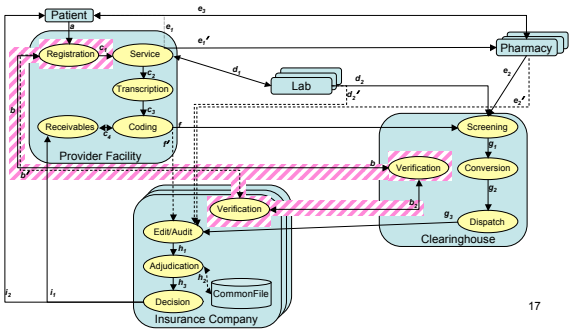
15

Medical Billing Network



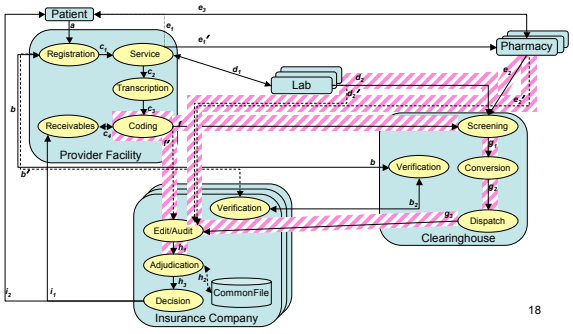
16

Medical Billing Network (Verify)



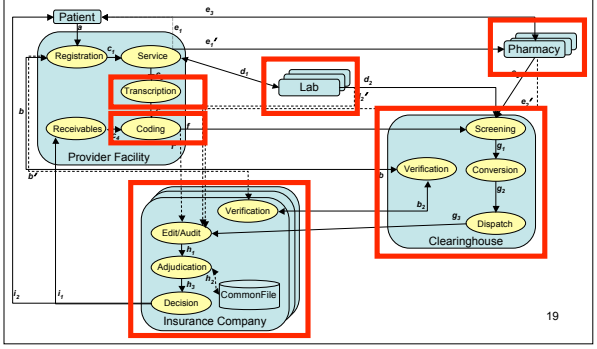
17

Medical Billing Network (Payment)



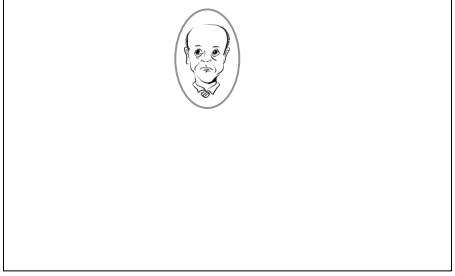
18

Medical Billing Network (Datasets)

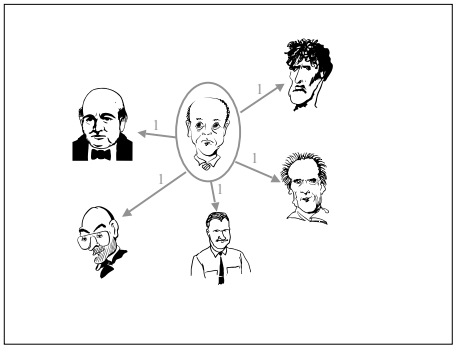


19

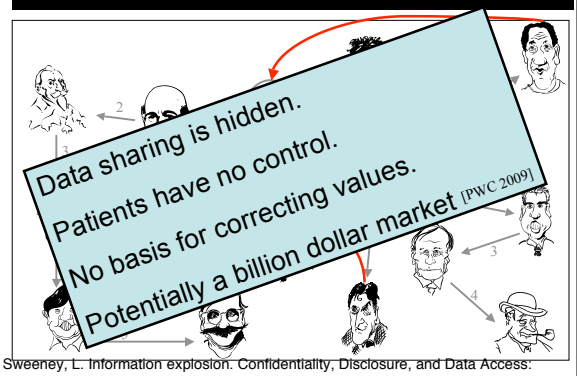
Original Data Holder



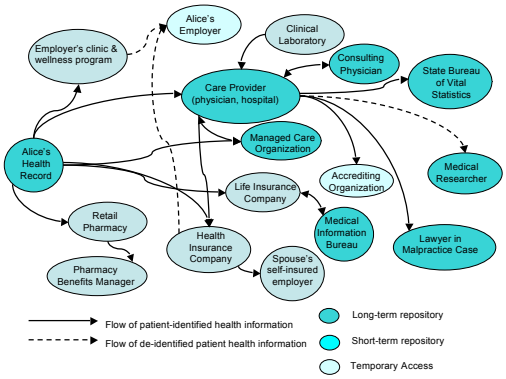
Primary Sharing MAY have some Restrictions



Secondary and Alternative Sharing Unbounded

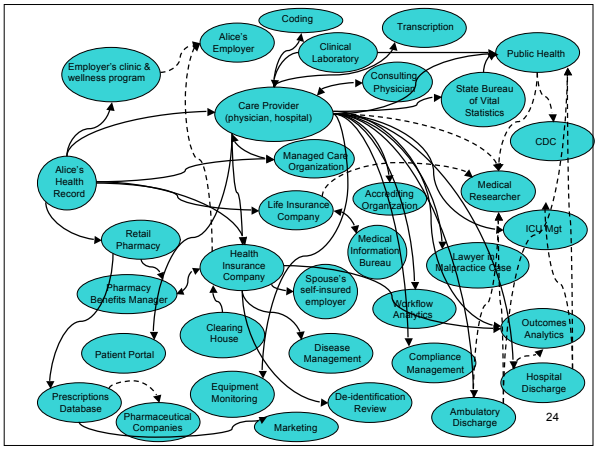


Sweeney, L. Information explosion. Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies, Washington, DC, 2001.



Clayton, P., et al. *For The Record.* National Academy Press,1997.

23

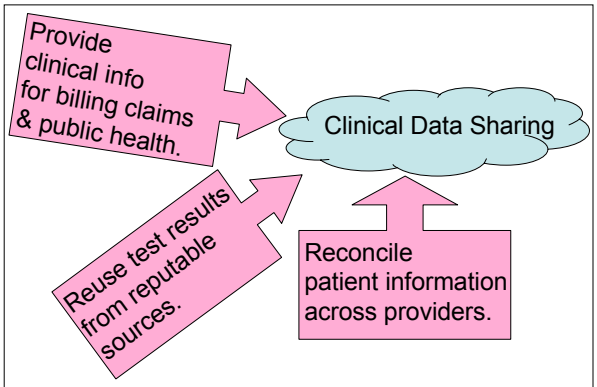


24

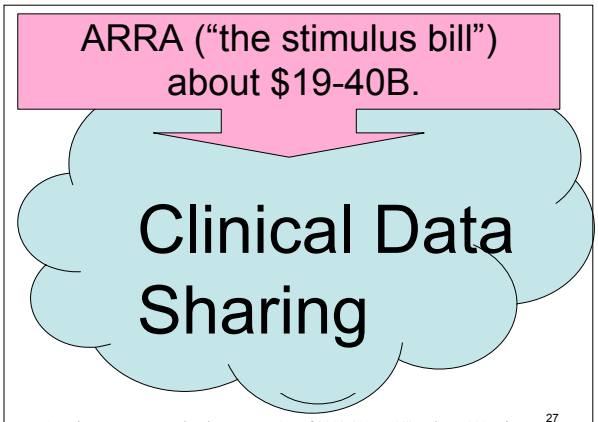
Given the power of technology design and the stimulus thrust to build the nationwide health information network (NHIN),

Explore trust issues in NHIN designs.

25



26



American Recovery and Reinvestment Act of 2009 ("ARRA") Pub. L. 111-5.â

27

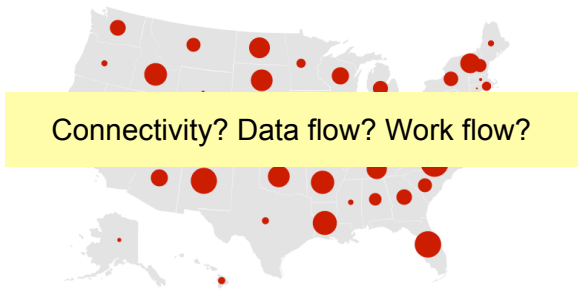
Meaningful Uses

- CBOE for medication, laboratory, diagnostic, imaging, etc.
  CMS quality measure: % of orders so entered.
- Implement drug-drug, drug-allergy, drug-formulary checks.
- Maintain and up-to-date problem, medication, and allergy list
- Check insurance eligibility.
  CMS measure: % patient with insurance eligibility confirmed.
- Submit claims electronically.
  CMS measure: % claims submitted electronically to all payers.
- Exchange clinical information (e.g. medication list, allergy list).
  CMS measure: exchange clinical info (e.g. medication list).

Federal HIT Policy Committee, Final Meaningful Use Objectives and Measures: 2011-2013 2015. At <healthit.hhs.gov>

28

Regional Exchanges



National Committee on Vital and Health Statistics. *Assuring a Health Dimension for the National Information Infrastructure: a concept paper*. Presented to the U.S. Department of Health and Human Services Data Council. October 14, 1998. www.ncvhs.hhs.gov/hii-nii.htm

29

1. How are records for the same patient identified as belonging to the same person?
2. What information is made available to which providers?
3. How is relevant patient information determined, consolidated and provided prior to the service?
4. How are data audits conducted?
5. How is data provenance established?
6. How are [illegible]?
7. [illegible] and sharing
8. [illegible] to the infrastructure and how are they [illegible]?
9. How [illegible] national health quality measures assessed?

… patient empowerment? … privacy?

Gap in readiness!

More about design solutions later in this talk.

Sweeney, L. *Background for Competitive Designs for the National Health Information Infrastructure.* Advance HIT Project. White Paper 1002. Carnegie Mellon. 2009.

30

Given the power of technology design and the stimulus thrust to build the nationwide health information network (NHIN),

Explore trust issues in NHIN designs.

31

Current ONC Design

Fax Common method today.

NHIN "Let 1000 weeds fester."

Miscommunication

Incompatibility ("chaos")

Inherit all privacy problems

yPage&parentid=18&mode=2&in_hi_userid=10741&cached=true

NHIN Limited Production Exchange

Operational Participants

Social Security Administration, Veterans Administration, Department of Defense, Kaiser, etc.

NHIN Connect

Software operations: (1) patient lookup; (2) document query; (3) document retrieval; (4) audit log query; (5) authorized case follow-up; and, (6) event messaging.

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1407&parentname=Communit yPage&parentid=18&mode=2&in_hi_userid=10741&cached=true 33

Current ONC Design

NHIN Connect

Software operations: (1) patient lookup; (2) document query; (3) document retrieval; (4) audit log query; (5) authorized case follow-up; and, (6) event messaging.

Insiders can do malicious survey to locate patients and patient records (e.g. domestic violence stalker).

34

Current ONC Design

NHIN Connect

Software operations: (1) patient lookup; (2) document query; (3) document retrieval; (4) audit log query; (5) authorized case follow-up; and, (6) event messaging.

3rd party automatic notification is outside direct patient care and allows unsupervised surveillance (e.g., notifications of abortions performed).

35

Current ONC Design

NHIN Connect

Software operations: (1) patient lookup; (2) document query; (3) document retrieval; (4) audit log query; (5) authorized case follow-up; and, (6) event messaging.

Local copies of patient data in environments having no professional staff to follow the latest computer security practices (and if certification by FDA required, machines may not be eligible for timely automated patches!).

36

NHIN Direct

Secure Email

Send email over secure channels to combat eavesdropping.

Cannot achieve all meaningful uses, so will need an additional system. For example, cannot get allergies and medications for an unconscious patient presenting at an out of state emergency room.

http://nhindirect.org/

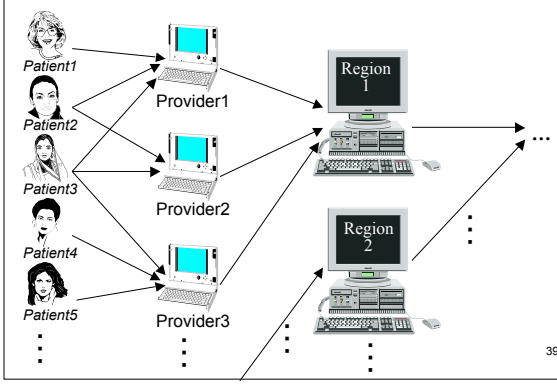
37

Given the power of technology design and the stimulus thrust to build the nationwide health information network (NHIN),

Explore trust issues in NHIN designs.

38

Deduplication & Identity



39

Deduplication & Identity

Aim

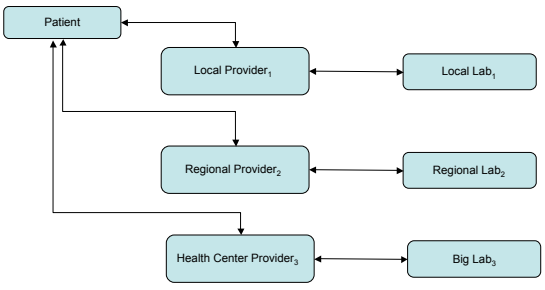
Goal is to get a distinct global count of patients matching a given criteria.

Complication

Common approach is to provide identifiers (e.g., patient SSNs) rather than counts so recipient can perform deduplication. This generates a privacy concern.

40

Testing & Liability



41

Testing & Liability

Aim

Goal is to reuse test results. Source must be reputable, image not modified, and belongs to the correct patient and is accurate. ("digital signatures")

Complication

Providers are concerned about liability. Credentials are not the same as a trustworthy relationship. If a provider acts on results, even in part, he increases his liability.

42

43

Corrections

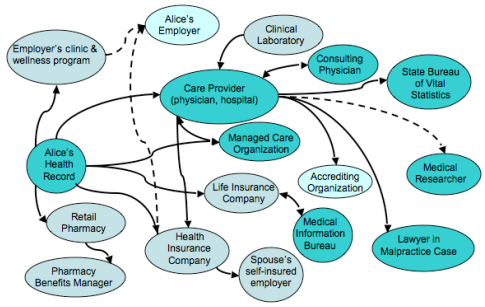
In the data sharing environments described so far, there is no mechanism for propagating corrections or updating information.

Concern

Can generate false information when incorrect data is in the result set.

44

Data Segmentation



45

Data Segmentation

Goal is to provide patients with some privacy protection by sequestering some data.

Concern

Generates an "inference problem" about data relations that may allow the missing information to be learned. Must be enforced across autonomous copies of related data held in different organizations.

46

Care & Safety

10/27/2005[2]	Pharmacy filled prescription for penicillin.
1/3/2009	Diagnosis of pregnancy
…	*… visits related to pregnancy*

Dr. Faye recommends an endocarditis prophylaxis and prescribes Biocef, orally. Life-threatening complications result because Eve did not remember, and Dr. Faye did not know, that Eve has a penicillin allergy with an immediate hypersensitivity reaction.

47

Care & Safety

Aim

Goal is use consolidated information over time and from different providers to improve decision-making for the patient.

Complication

Need to decide whether a particular piece of data should be in the result set, whether it should be valued, or whether data may be missing.

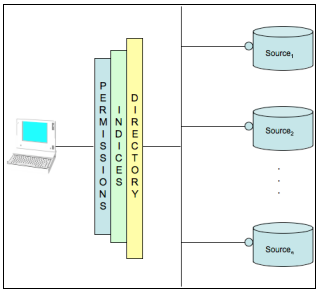
48

Given the power of technology design and the stimulus thrust to build the nationwide health information network (NHIN),

Explore trust issues in NHIN designs.

49

Design Pattern 1: Global Query



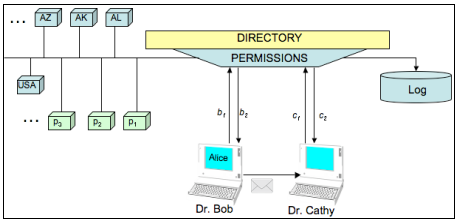
Answer queries across a collection of repositories in real-time, providing the same answer as if all data were centralized.

Analogy: web searching.

Also: numeric results, e.g. counts, regressions, and percentages. Another form of query is data extraction.

50

Design Pattern 2: Certified Delivery

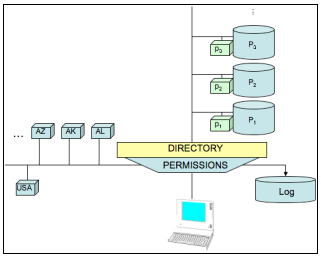


Point-to-point delivery of health information with verifiable and accountable endorsements of sender and receiver per contents.
Analogy: email and fax .

Centralized (design 1) or de-centralized services (above).

51

Design Pattern 3: Patient Central



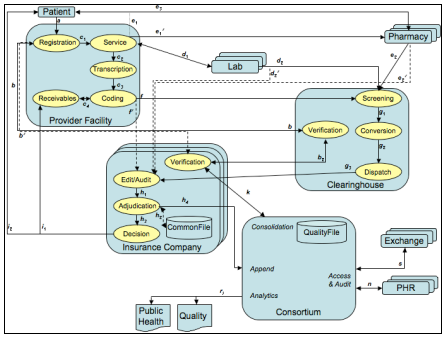
Uses globally available storage of patient information arranged by patient.

Analogy: file cabinet.

An EMR not “patient health record” (PHR).

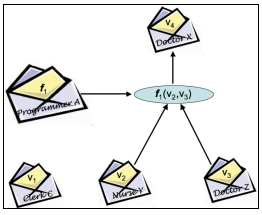
52

Design Pattern 4: Medical Billing Backbone



53

Design Pattern 5: Heavy Data



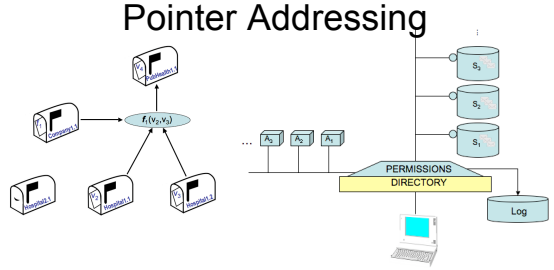
Tethers or embeds meta-information along with data values. Meta information travels with data.

“Dependency tracking model” adds retrospective accountability. (shown)

“Sticky policies” affixed to data values to represent data sharing allowances, prohibitions and consents.

54

Design Pattern 6: Pointer Addressing



Share published network addresses of data rather than data values themselves.

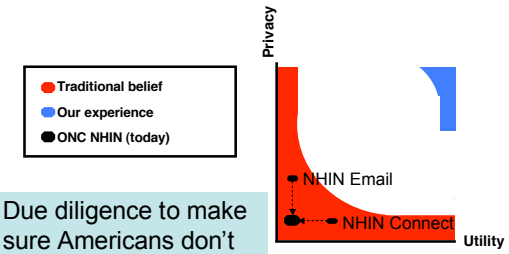
Pointer addressing (left) and its use with heavy data using grid computing technologies (right).

55

Design Patterns	Issues
1. Global Query	• Deduplication & Identity
2. Certified Delivery	• Testing & Liability
3. Patient Central	• Care & Safety
4. Medical Billing	• Data Segmentation
5. Heavy Data	• Corrections
6. Pointer Addressing	• …

56

Information ~~Or~~ And Privacy



Due diligence to make sure Americans don't settle for loss of privacy or performance.

57

Technical Way Forward

1. Identify utility requirements and critical stakeholder barriers.
2. Assess each design pattern in light of the utility requirements and stakeholder barriers.

#1 provides a common criteria any design much achieve to be acceptable for use.

#2 gives decision-makers, advocacy groups, and developers shared knowledge to assess designs.

58

ADVANCEHIT

Trustworthy Designs for the Nationwide Health Information Network

Latanya Sweeney, PhD
Harvard University, MIT, Carnegie Mellon University

59

latanya@seas.harvard.edu AdvanceHIT.org

60