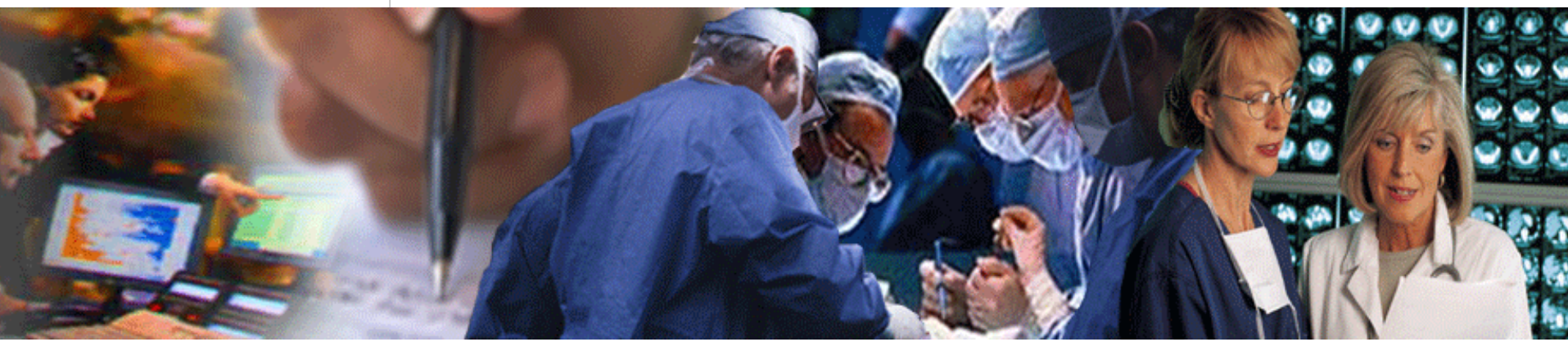
2nd Nationwide Health Information Network Forum:
Health Information Network Security and Services

October 16-17, 2006

Panel Discussion

Patient Driven Access Control

Vinod Muralidhar
Computer Sciences Corporation
Connecting for Health NHIN Team



EXPERIENCE. RESULTS.

Patient Driven Access Control

Patient Control of Access to their own Healthcare Data

- **PROS**
  - Presumed *sine qua non* of 'consumer-centered' health information networks
  - Patient has reasonable expectations of confidentiality and care in the handling of their data, and should be able to ask that data be shared:
    - » only with other organizations that have a legitimate need for, and right to, the data.
    - » with someone acting as their proxy, and that they can later revoke that access.
    - » with a clinician or organization, but that those organizations be denied access in the future.

Patient Driven Access Control

Patient Control of Access to their own Healthcare Data

- **CONS**
  - Adding consumer control of the data is
    - Technologically challenging
    - Expensive
    - Proper use requires savvy consumer
    - Challenges in integrating with provider workflows
  - Current systems and network architectures not conducive to
    - granular partitioning of data
    - per-access consent
    - revocable data
    - complex rule-based access
  - Are consumers equipped to handle access control responsibilities?
    - Do they have insight into implications (informed consent?)
    - Consumers don't know enough about the data to make choices at a granular level
    - Chronic care patients have shown little interest in access control – higher priority on providers having access to all relevant data

Patient Driven Access Control

Types of Data Consumers Want to Control Access of

- **Average consumer expected to want to control**
  - Mental health related data
    - Need to be careful not to define this too broadly or you begin to erode the utility of clinical data in general
  - HIV data
- **CONS**
  - Medical data is multi-faceted and semi-structured
    - Impossible to partition "facts" about a patient
  - HIV status can be derived from declaration of status, current drug regime; chief complaint; diagnostics; planned tests; or doctors notes
  - Partitioning strategies can only be applied to categories (types of providers, or drugs), and only on data that is both clean and well organized
  - Early patient controlled health records have tried to be proactive
    - PatientSite waits one week before notifying patients of cancer / HIV results, allowing care giver to communicate first
    - Restricted access to progress notes

Patient Driven Access Control

Propagation of User Preferences across Network

- **PROs**
  - Distributed data requires distributed management (complex)
  - Effective patient driven access control calls for propagation of control to all locations where data exists
- **CONS**
  - Data once released from primary source cannot be really be controlled without data management investment that is proportional to scale of the network
    - Clinical and regulatory practice prevents a data-holder from deleting it
      - » Cannot implement revocability in current environment
  - Control is effected through applications and not ‘encapsulated’ with the data
      - » You can control applications not data
  - Media industry has spent $billions on Digital Rights Management to little lasting effect

Patient Driven Access Control

Steps/Levels where Preferences could be Implemented

- **Patient management of access control may occur at many places in network**
  - Control is best effected through applications at the edges and not “in the network”
  - PHRs / Patient portals offers logical choice as primary point of control
  - Current EMRs do not allow direct patient access, but contain the most healthcare data
- **CONs**
  - Need to propagate access control information
    - Propagating access control results in significant complexity
    - Once information has been “released” in compliance with the patient’s desired access controls then its disposition becomes governed by other rules and regulations
  - Mechanics of patient assigning permissions to individual providers require means to identify roles / individual providers
  - Individual providers practically almost impossible to enumerate or even know in advance

Patient Driven Access Control

Data Exchanges Necessary to Implement Access Controls

- **Full access control capability requires sharing of**
  - Subjects: Individual and Organizational Providers, Roles
  - Resources: Patient data, Data types and domains
  - Actions: Read / Write / Update
  - Rules: Permit / deny based on conditions
- **PROs**
  - Distributed access control management across network nodes
- **CONs**
  - High complexity solution requiring significant synchronization of security architectures across multiple enterprises
  - Likely too complicated to implement in reasonable time frame

Patient Driven Access Control

Minimizing Impact on Providers delivering Patient care

- **PROs**
  - Authority resides with ultimate information owner/steward of information, who has the most interest in it
  - Focusing the control points to the source where the patient and provider can have a shared dialog about access control is ideal

- **CONs**
  - Consumers unaware of potential impact on their own healthcare of controlling (denying) care givers access to their health information
  - As copies proliferate, impossible to locate all versions of data pertaining to a particular patient, or all copies of a particular piece of data
  - Without 'Break-the-glass' function can be hazardous to healthcare in the foreseeable future