Primary Care Coalition of Montgomery County, MD
Center for Community-Based Health Informatics
8757 Georgia Ave, 10th Floor, Silver Spring, Maryland 20910

National Committee on Vital and Health Statistics

Subcommittee on Privacy and Confidentiality

Testimony by Primary Care Coalition of Montgomery County, Md

Thomas L. Lewis, MD
Erin N. Grace, MHA
Guy G. Fisher
June 7, 2005

Primary Care Coalition of Montgomery County, MD

- A non-profit focused on improving access to quality health for the 80,000 uninsured in our county
    - Working with the 10 independent safety net clinics in the county, one in DC and plans to add at least one in Northern Virginia
    - Helping the county government provide for the uninsured
- Leveraging IT, through our Center for Community-Based Health Informatics
    - With a HRSA HCAP grant, implemented a single, shared Electronic Health Record system for the clinics to form a virtual system of care – now handling 80% of the county's safety net visits (25,000 per year)
    - With an AHRQ Planning grant, we are planning the interconnection of our shared EHR and others in metro DC with mainstream health care
    - My role -- Principal Investigator
    - My background – MD with Public Health Service; 34 years with NIH; CIO of NIH Clinical Center research hospital; now with PCC

Healthcare Privacy and Confidentiality in the electronic world have been our concerns as we've been building a mini Safety Net "RHIO" from scratch

Privacy for Personal Health Data is a new and different challenge

- Disclosure of Personal health data can't be rescinded! Damage is permanent!
  - DNA testing of railroad workers for carpal tunnel potential
  - Job loss/denial due to pre-existing conditions, psychiatric history
  - Health and Life insurance discrimination
  - Social ostracism
  - The oft used quote "No one ever died from release of their medical data" is wrong
- Any analogy to Financial Data privacy misses the mark
  - Not reversible, as with financial "identity theft"
  - Money is recoverable, records can be corrected, accounts can be changed
- Recent ChoicePoint and LexisNexis identity thefts show:
  - Vulnerabilities
  - Perception of enterprises not held accountable for lapses in data security
  - Lack of government role in regulating disclosure of personal data
  - Greatly diminishes trust of "the system"
- "Just as private as Financial Data" isn't good enough

Building and Earning Trust is the key – continuing disclosures of personal financial data destroy the trust we need

We can learn from the UK experience

- The UK NHS research found both:
  - **trust –** "High level of trust" in NHS by citizens, and
  - **skepticism** – only 8% would want to put "a lot or all" of their health information in a shared electronic health record
  - What does that say about the Trust hurdles in the US?
- UK's attempt at reducing skepticism -- "Care Record Guarantee"
  - Reasonably clear statement of use: those in need to know for healthcare, specifically excluding others in UK government
  - Patient control over use: Assent and Dissent, with NHS Dissent Override for others' safety
  - Patient control of fine grained access
    - What the dentist can see is more limited than the heart surgeon

We have a start with HIPAA, but…

- Is it clearly understood by our residents?
- Does it address fine grain access control by patients sufficiently?
- Has it helped build the needed trust?

The Federal government has a crucial role to play in laying foundation for TRUST

Early Experiences with Safety Net "RHIO"

- Data sharing is considerably more critical for the uninsured
  - Patient-specific factors
    - Patients choose multiple providers,
    - Less likely to declare a Medical Home
    - Significant use of Emergency Departments for primary care
    - Care site changes driven by
      - Migrant workers across region
      - Frequent job changes within region
      - Frequent housing changes
  - Clinic-specific factors
    - Volunteer providers, infrequent hours
    - Part-time clinics
  - Examples:
    - Expensive, dangerous workup in one ED repeated one week later in a second ED
    - Medications shopping across multiple clinics and ED's
    - Patients seek care in multiple jurisdictions concurrently
    - High likelihood that caregiver is different at each visit

Data sharing more critical for Quality of care for Uninsured

Early Experiences with Safety Net "RHIO"

- Trust is more difficult to establish
    - Lack of close relation between patient and primary care giver
    - Cultural bias towards distrust of "the system"
    - Immigration status often prevents openness, enhances concern over use of data
    - More difficult to convey the benefits message, to build trust
    - Language and educational barriers (why dentist must have HIV data)
- Adverse consequences of distrust
    - More likely to forego needed treatment, requiring more expense later
    - Increased risk to public health if people won't share their health data
- Recent experience:
    - Voluntary approach to sharing seems to be working
        - For established patients at established clinics
        - Less so in other settings, e.g. Emergency Departments
- We're charting new territory – no single point for assistance
    - PCC developed sharing agreement suite for multiple jurisdictions

More difficult to build trust and therefore to share data

Early Experiences with Safety Net "RHIO"

- Automated matching is less reliable and more problematic
  - No insurance ID
  - Patient not in Pharmacy Benefits Manager database
  - Cultural naming conventions lead to multiple representations
  - Frequent changes of address and phone number
  - Unknown Birth date
  - Multiple occurrences of the same patient even in the same clinic database
- Multiple matching algorithms being used and developed
  - May be less reliable in the safety net population
  - Certainty of match essential for patient safety
  - Omissions and false inclusions are both likely
- Example of contributory factors:
  - Frequent moves
  - Overcrowded rental, so does not give valid address
  - Borrowed IDs

Local Patient-Centric Trust Building – Key to sharing of health information

Privacy and the RHIO – Global Considerations

1. The key stakeholder for privacy/confidentiality is The Patient, not the healthcare enterprises

2. Yes, it’s great to start by taking small steps …
   - Gradually build up EHR implementations
   - Gradually interconnect health systems

   … but implement Privacy, fully, at the beginning – risk of doing otherwise is too great

3. Privacy Framework should be national, implemented locally

4. Build patient Trust:
   - Clearly worded Guarantee
   - Clearly understood, and tough, penalties
   - Patient control of fine-grained access rights

Maintain Patient–Centric Focus

Privacy and the RHIO – Safety Net Challenges

- Data sharing is considerably more critical for the uninsured
- More difficult to build trust and therefore to share data
- Automated matching is less reliable and more problematic

Maintain Patient–Centric Focus. Extra effort required.