Connecting Americans to Their Health Care:

Empowered Consumers, Personal Health Records and Emerging Technologies

NATIONAL CONFERENCE
DECEMBER 7-8, 2006
WASHINGTON, D.C.

Connecting Americans to Their Health Care:

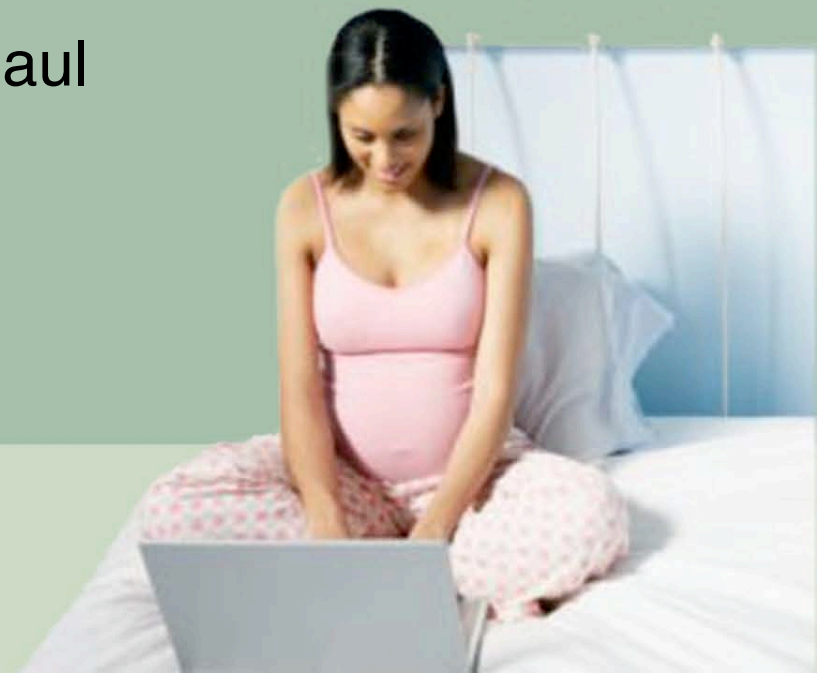
Empowered Consumers, Personal Health Records and Emerging Technologies

2006

Policies 101

Melissa M. Goldstein - The George Washington University Medical Center

Mark Frisse - Vanderbilt University Paul Feldman - Health Privacy Project



MARKLE FOUNDATION

Robert Wood Johnson Foundation

Connecting Americans to Their Health Care:
Empowered Consumers, Personal Health Records and Emerging Technologies

2006

Policies 101: Overview of the Connecting for Health Common Framework

Melissa M. Goldstein, JD
The George Washington University Medical Center

MARKLE FOUNDATION

Robert Wood Johnson Foundation

What is Connecting for Health?

- A public-private collaborative of 100+ organizations representing all the points of view in healthcare
- A neutral forum
- Founded & supported by the Markle Foundation
- Additional support from the Robert Wood Johnson Foundation

What is the Purpose of Connecting for Health?

To catalyze changes on a national basis to create an interconnected, electronic health information infrastructure to support better health and healthcare

Healthcare is Different

- The healthcare system is very diverse
- Health information is especially sensitive—and privacy spills can't be "fixed"
- Patients/consumers are traditionally less involved than in some other areas

Some Barriers to Electronic Information Sharing in Health

- Technical (e.g., lack of standards)
- Policy (e.g., lack or incompatibility of rules about who is allowed to see information and why)
- Financial (e.g., misalignment of incentives for IT adoption)
- Educational (e.g., lack of understanding of the benefits and risks of IT)

… and the technology is the *easy* part!

Sharing Health Information = Linking Existing Sources

- Health information can *stay where it is*—with the doctors and others who created it
- Specific information is shared *only* when and where it is needed.
- Sharing *does not* require an all new "network" or infrastructure
- Sharing *does not* require a central database or a national ID
- Sharing *does* require a Common Framework

A Common Framework Is Needed

- The Common Framework is the minimum necessary set of rules or protocols for *everyone* who shares health information to follow
- Helps organizations overcome the barriers without "reinventing the wheel"
- Enables nationwide interoperability…avoiding isolated islands of information
- Builds *trust*

Overview of Connecting for Health Architecture

- A sub-network organization (SNO) brings together a number of providers and other health information sources
- They are linked together by contract
- Agree to follow common policies and procedures
- Agree to create and use a shared index to where patient records are located (RLS)
- Agree to create and use a common gateway to share information with other networks (ISB)

What is a Record Locator Service (RLS)?

- An index containing patient demographic information and the location of a patient's medical records
- Contains no clinical information – obtaining the clinical record is a separate transaction NOT involving the RLS
- Participating entities decide whether or not to put record locations into the RLS
- Designed to take a query in the form of demographic details and return only the location of matching records

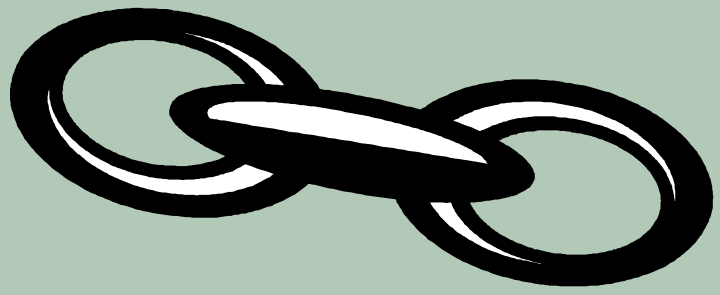
How Was the Common Framework Developed?

Connecting for Health…

- Started with Design Principles
- Wrote a Roadmap in 2004
- Built a Prototype
- Developed the Common Framework through field experience and the collaboration of experts

Technology and Policy are Intertwined

- Choices about one necessarily shape the other
- To build trust, you have to put policy decisions first



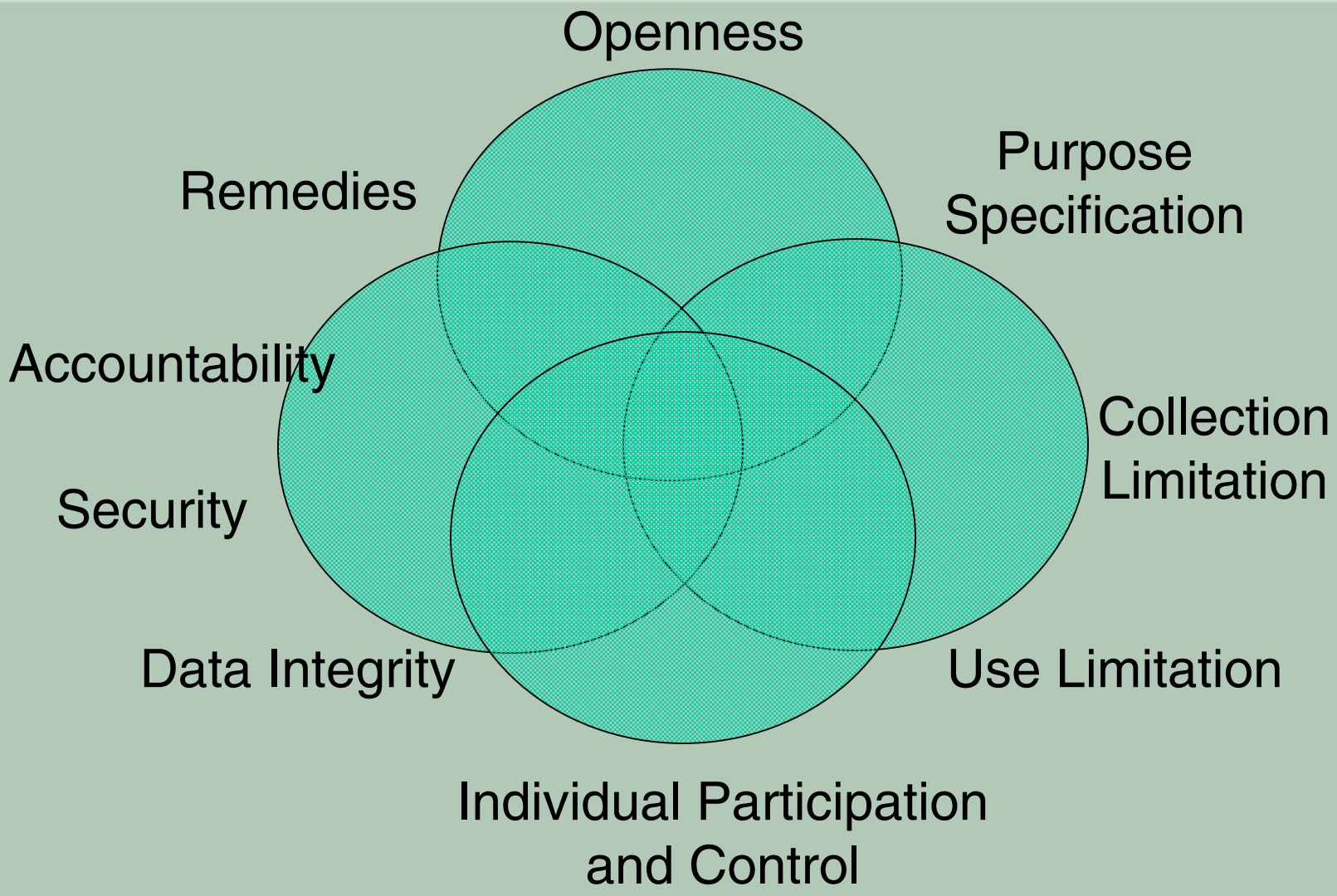
Technical Principles

1. Make it “Thin”
2. Avoid “Rip and Replace”
3. Separate Applications from the Network
4. Decentralization
5. Federation
6. Flexibility
7. Privacy and Security
8. Accuracy

Privacy Principles

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. Data Integrity and Quality
7. Security Safeguards and Controls
8. Accountability and Oversight
9. Remedies

The Privacy Principles are Interdependent



The Prototype

- Three sites
  - Boston: MA-SHARE and technical partner CSC
  - Indianapolis: Regenstrief Institute and Indianapolis Health Information Exchange (IHIE)
  - Mendocino County, CA: Mendocino HRE and technical partner Browsersoft, Inc.
- Diverse architectures
- Diverse structures

If these 3 can all use the Common Framework…anyone can!

Who Developed the Prototype and the Common Framework?

- Connecting for Health Steering Group
- Policy Subcommittee: Co-Chairs Bill Braithwaite and Mark Frisse
- Technical Subcommittee: Chaired by Clay Shirky
- Three communities and teams:
  - **Boston**
  - **Indianapolis**
  - **Mendocino**

Connecting for Health Policy Subcommittee

- About 40 experts in
  - Law
  - Health privacy and ethics
  - Health care delivery
  - Administration
  - Technology
  - Local network development (RHIOs)

Connecting for Health Policy Subcommittee

- Looked at HIE in the context of HIPAA and existing state laws
- Developed a list of significant topics from
  - Members' experience with early information exchange networks
  - Members' own expertise

Challenges Addressed by Policy Subcommittee

- Who has access to what, under what circumstances, and with what protections?
- Who shares what and who bears the liability?
- How can you control access to your information?

Policy Subcommittee Goals

- Develop a policy framework
- Identify what needs to be common for interoperability and what does not
- Develop a working guide

What Do the Common Framework Resources Consist of?

- Technical rules and standards—that allow systems to “talk to” each other
- Policies on how to handle information– that build *trust*
- Model contractual language—that holds it all together

What is Available?

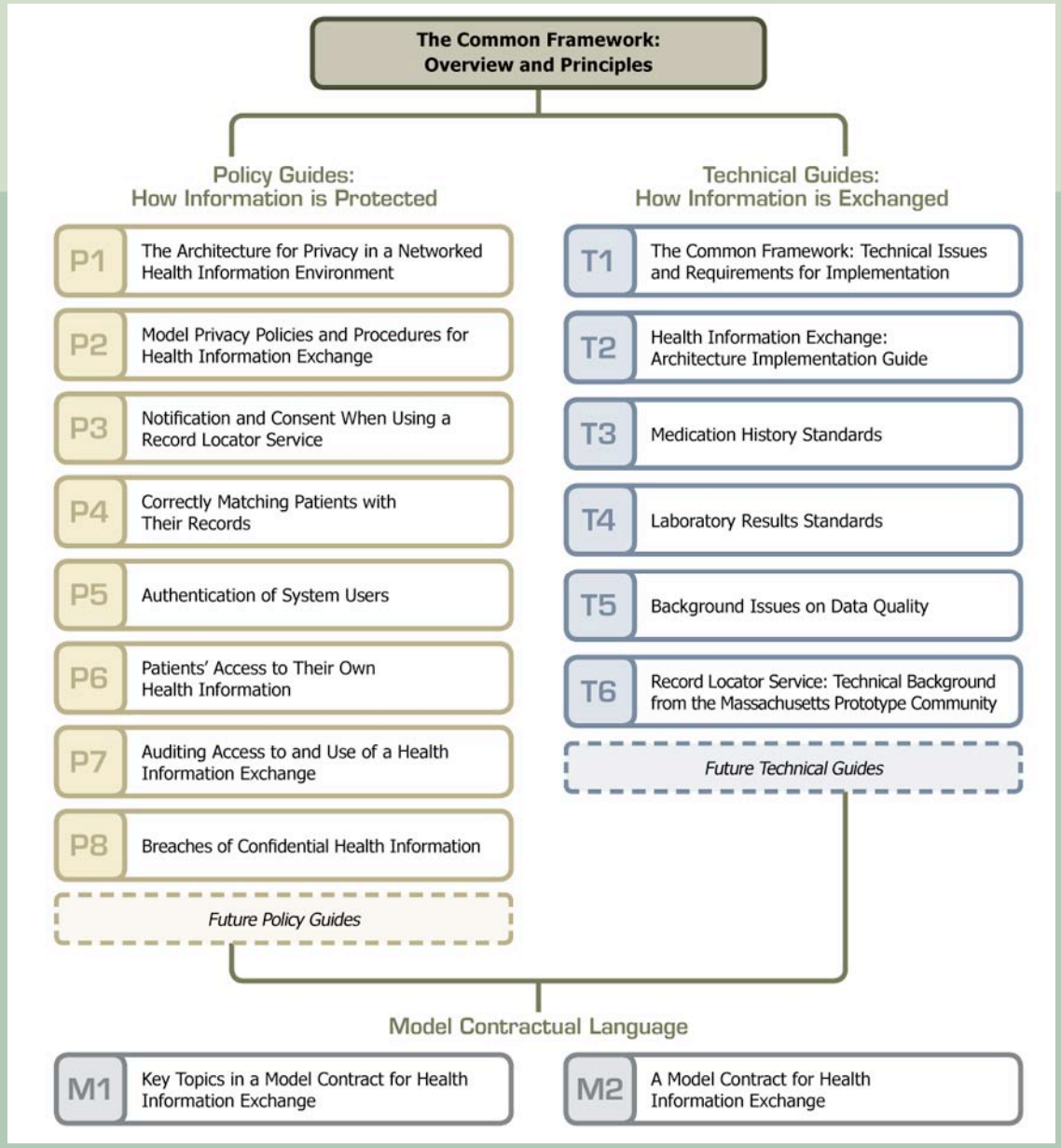
Technical Documentation: 3 Categories

1. Background Documents
   - T6: Record Locator Service Design
   - T5: Data "Cleanliness" and Quality
- Specific Technical Documents
   - T1: Technical Overview and Implementation Requirements
   - T2: NHIN Message Implementation Guide (Record Locator Service/Inter-SNO Bridge)
   - T3-T4: Standards Guides
     - Medication History: Adapted NCPDP SCRIPT
     - Laboratory Results: ELINCS 2.0, with modifications
– Technical Code and Interfaces
   1. Test Interfaces: CA, IN, MA
   2. Code base: CA, IN, MA

What is Available?

Policy Documents: 3 Categories

1. Background Document
   - P1: Privacy Architecture for a Networked Health Care Environment
- Specific Policy Documents
   - P2-P8: Model privacy policies, notification and consent, correctly matching, authentication, patient access, audits, and breaches
- Sample Contract Language
   - M1: Contact Topic List
   - M2: Model Contract



Connecting Americans to Their Health Care *2006*

Sample Policy Documents

Sample policy language

CFH Recommended policy

Incidents to the covered entity.[13] *See relevant sample contract excerpts below:* [14]

Section 8.03 Report of Improper Use or Disclosure. [The SNO] agrees promptly to report to a [Participant] any use or disclosure of the [Participant's] PHI not provided for by this Agreement of which [the SNO] becomes aware.

and

Section 8.14 HIPAA Security Rule Provisions.

(a) ...
(b) [The SNO] agrees promptly to report to a [Participant] any Security Incident related to the [Participant's] ePHI of which [the SNO] becomes aware.

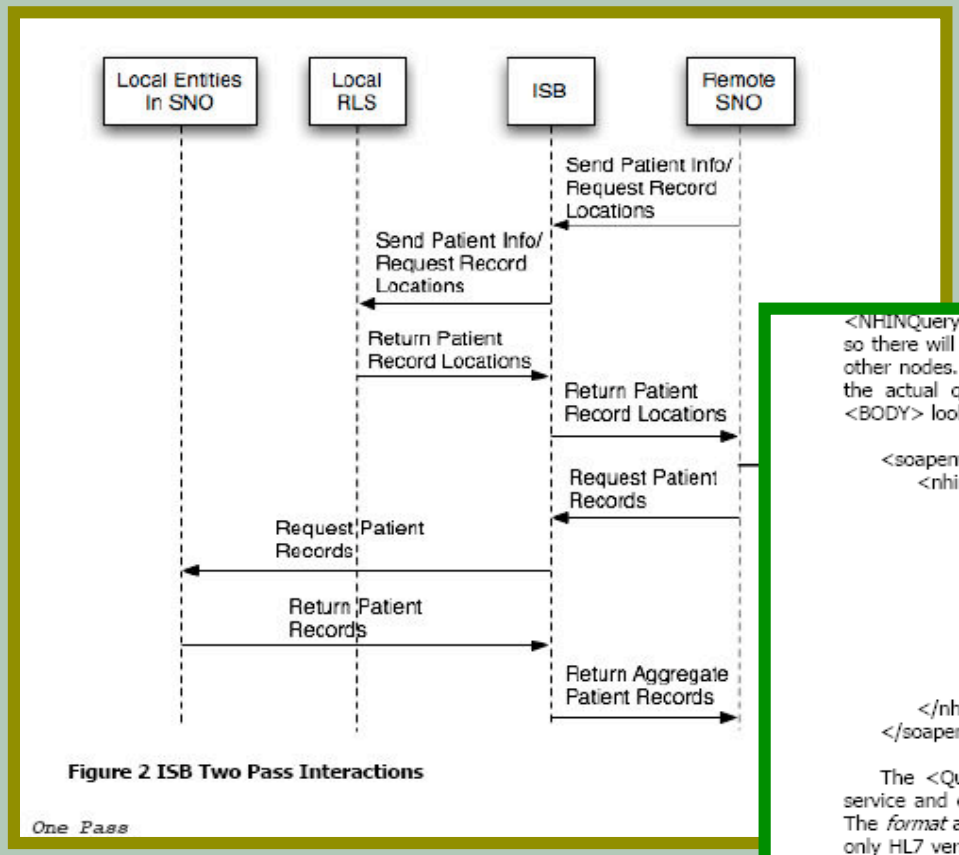
Similarly, each Participant must agree to inform the SNO of any serious breach of confidentiality. It is not necessary for a Participant to inform the SNO of minor breaches of confidentiality (unless there is otherwise a legal duty to disclose such breaches to the SNO). While it is difficult to define what would rise to the level of a "serious" breach, SNOs and Participants might decide that the breaches of

From P8 – Breaches, p. 4

Model Terms and Conditions	Notes
4.7 Participant's Other Rights to Terminate Registration Agreement. *How a Participant may cease to be a Participant, generally.* **Alternative One: Participant may terminate at any time without cause.** A Participant may terminate its Registration Agreement at any time without cause by giving notice of that termination to [SNO Name]. **OR** **Alternative Two: Participant may terminate without cause with prior written notice.** A Participant may terminate its Registration Agreement at any time without cause by giving not less than _____ days prior notice to [SNO Name]. **OR** **Alternative Three: Participant may terminate as of the next anniversary of having entered into the Registration Agreement.** A Participant may terminate its Registration Agreement at any time without cause effective as of the next anniversary of the effective date of the Participant's Registration Agreement, by giving not less than _____ days prior notice to [SNO Name]. **OR** **Alternative Four: Participant may terminate for cause (may be combined with Alternatives Two or Three and/or Five).** A Participant may terminate its Registration Agreement upon [SNO Name]'s failure to perform a material responsibility arising out of the Participant's Registration Agreement, and that failure continues uncured for a period of sixty (60) days after the Participant has given [SNO Name] notice of that failure and requested that [SNO Name] cure that failure. **OR** **Alternative Five: Participant may terminate for specified cause (may be combined with Alternatives Two or Three and/or Four).** A Participant may terminate its Registration Agreement upon a Serious Breach of Confidentiality or Security, as described in Section 9.3 (Reporting of Serious Breaches), when such Serious Breach of Confidentiality or Security continues uncured for a period of sixty (60) days after the Participant has given [SNO Name] notice of that failure and requested that [SNO Name] cure that breach.	The SNO may wish to allow Participants to terminate their participation freely at any time, or to require that termination be preceded by a substantial period of advance notice, or to require that Participants maintain their participation for a year (or longer) at a time. If the SNO wishes to limit further certain Participants' (*e.g.*, certain data providers) rights to terminate their participation, the SNO may provide for such special terms in written Registration Agreements described in Section 4.2 (Registration by Agreement). If the SNO places limits upon the Participant's right to terminate, the SNO may wish to provide for the Participant's right to terminate based on the SNO's failure to perform. The Model provides a simple "termination for cause" provision. The SNO may wish to qualify a Participant's right to terminate, *e.g.*, by providing in addition that if the SNO's failure to perform is one that the SNO cannot reasonably cure within the specified period, then the termination will not take effect so long as the SNO commences and diligently pursues work to cure the failure.

From M2 – Model Contract, p. 10

Sample Technical Documents (T2)



<NHINQuery> node. The WS-Basic Profile 1.0 requires a single node within the SOAP <BODY>, so there will never be a second node at this level. Within the <NHINQuery> node, we find two other nodes. One contains control information about the query settings and the other contains the actual query. For example, the topmost level of the *PatientDataQuery* SOAP message <BODY> looks like:

```
<soapenv:Body>
    <nhin:NHINQuery>
        <nhin:EvaluationSettings>
            <nhin:MaxResponseInterval>60</nhin:MaxResponseInterval>
            <nhin:ResponseStyle>I</nhin:ResponseStyle>
        </nhin:EvaluationSettings>
        <nhin:Query format="HL7" version="2.4">
            <QBP_Z01 xmlns="urn:hl7-org:v2xml">
                ...
            </ QBP_Z01 >
        </nhin:Query>
    </nhin:NHINQuery>
</soapenv:Body>
```

The <Query> node defines the information that is actually being requested. The SOAP service and operation are merely wrappers in which to pass this generic "query" specification. The *format* and *version* attributes define the format in which the query is expressed. Currently, only HL7 version 2.4 queries are supported. NHIN is considering support of HL7 version 3.0 as its use becomes more widespread.

At the topmost level of the SOAP message <BODY>, each response message also contains a single node. The <NHINResponse> node contains two data-bearing nodes, just like the

The Common Framework is Not a "RHIO in a box"

- It provides different models to consider—not one "right answer."
- It is intended as a partial solution. It does not address finance, governance, etc.
- There are topics (like how to aggregate data for research and public health) that Connecting for Health is still working on…

The Common Framework is Still Evolving

- Improving the resources to better meet the needs of communities
- Exploring how patients/consumers can access their own information (this conference)
- Exploring how researchers and public health can benefit from health data
- Connecting for Health needs the input of organizations nationwide….

Common Framework Resources

- All available free at www.connectingforhealth.org
- Policy and technical guides, model contractual language
- Registration for AHRQ/NORC Common Framework discussion forum
- Software code from regional prototype sites: Regenstrief, MAShare, OpenHRE
- Email to info@markle.org

Connecting Americans to Their Health Care:

Empowered Consumers, Personal Health Records and Emerging Technologies

2006

Policies 101

Mark Frisse

Vanderbilt University

MidSouth eHealth Alliance

Funding: AHRQ Contract 290-04-0006;
State of Tennessee; Vanderbilt University
This presentation has not been approved by the
Agency for Healthcare Research and Quality

MARKLE FOUNDATION

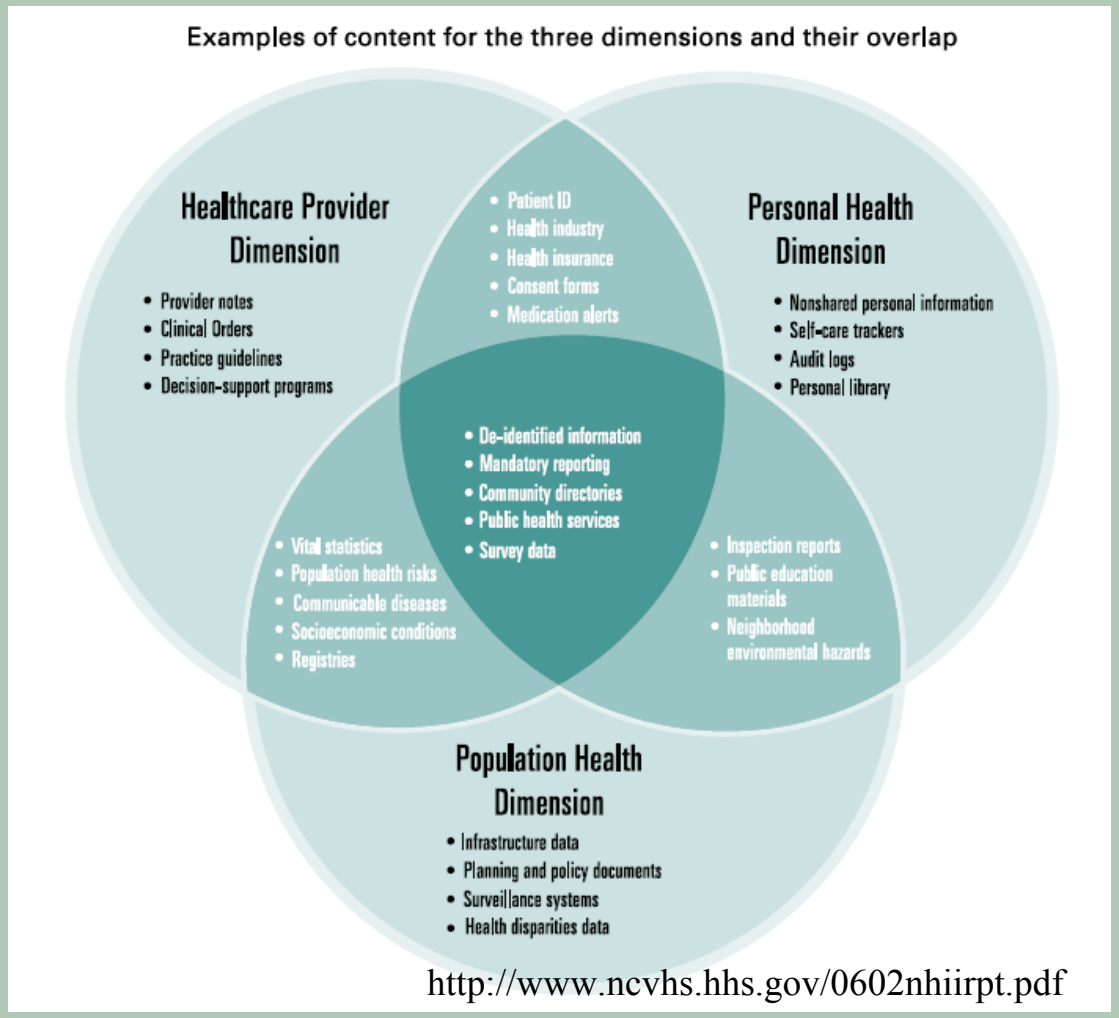
Robert Wood Johnson Foundation

What is a PHR?

http://www.ncvhs.hhs.gov/0602nhiirpt.pdf

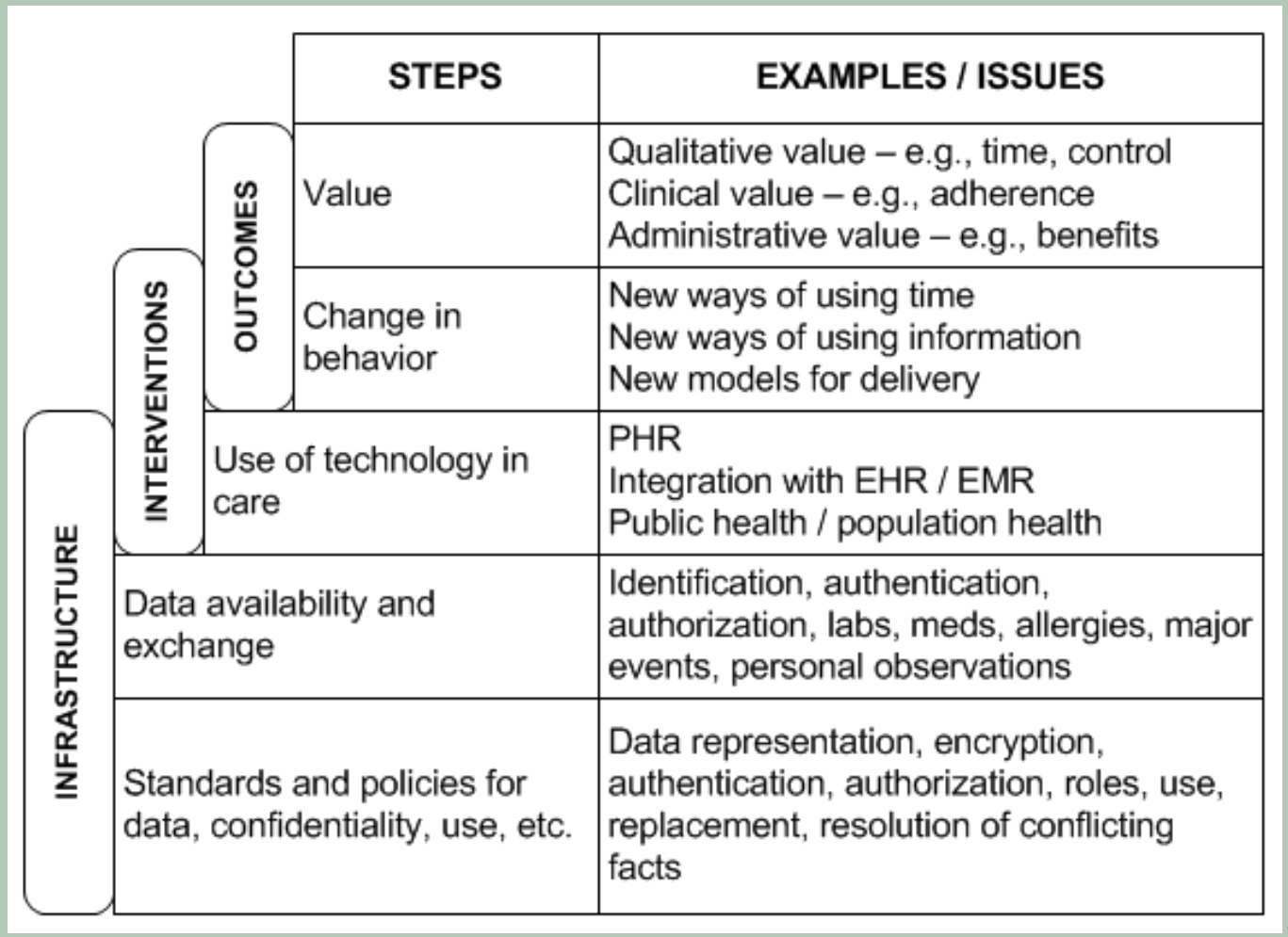
- NCVHS proposes adopting the term "personal health record" to refer to the collection of information about an individual's health and health care, stored in electronic format
- The term "personal health record system" refers to the addition of computerized tools that help an individual understand and manage the information contained in a PHR

Three dimensions of access



http://www.ncvhs.hhs.gov/0602nhiirpt.pdf

An intervention framework for personal health



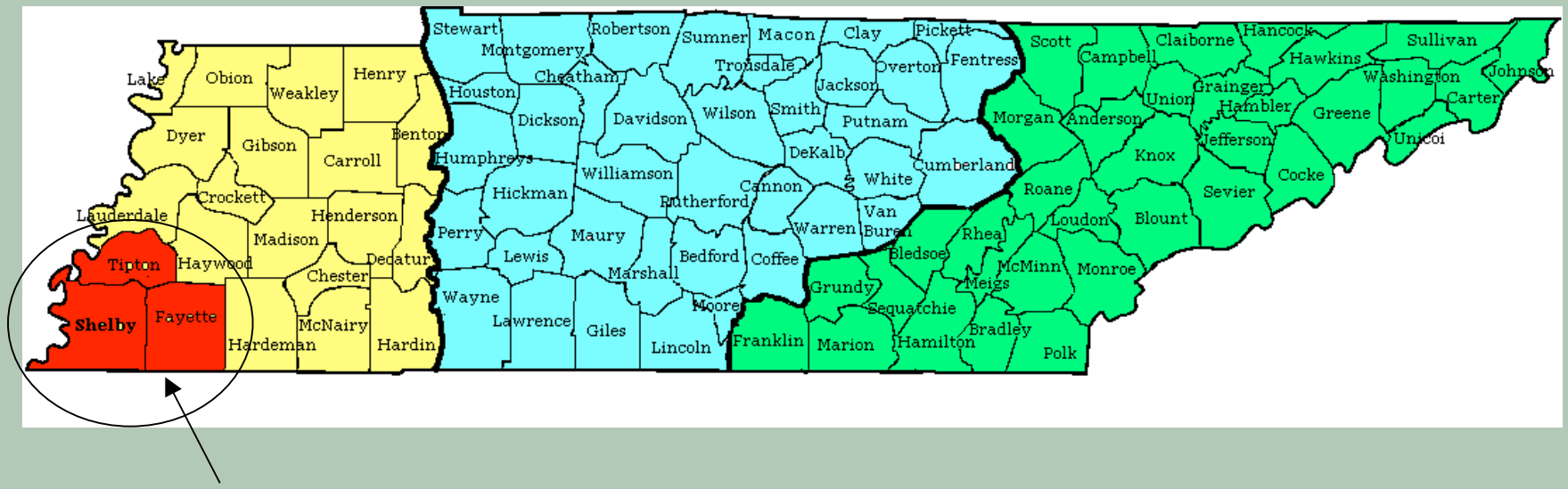
		STEPS	EXAMPLES / ISSUES
INFRASTRUCTURE	INTERVENTIONS	OUTCOMES: Value	Qualitative value – e.g., time, control Clinical value – e.g., adherence Administrative value – e.g., benefits
		OUTCOMES: Change in behavior	New ways of using time New ways of using information New models for delivery
	Use of technology in care		PHR Integration with EHR / EMR Public health / population health
	Data availability and exchange		Identification, authentication, authorization, labs, meds, allergies, major events, personal observations
	Standards and policies for data, confidentiality, use, etc.		Data representation, encryption, authentication, authorization, roles, use, replacement, resolution of conflicting facts

Vanderbilt AHRQ 2004 Proposal: Adapted from http://www.volunteer-ehealth.org/pdfdocs/AHRQ-10-30-04.pdf, p 10

Questions

- What lessons have we learned from functioning health information exchanges?
- How can these exchanges relate to personal health records in terms of:
  - Policies (e.g., confidentiality, use)
  - Technologies
  - Models for clinical care
  - Outcomes

One million people in three counties



Tennessee borders 8 other states

Our initiative covers 3 counties and includes Memphis.

11% of one TennCare population visited more than one ED in a year

20 – 25% of hospital visits in Memphis are from Mississippi or Arkansas residents

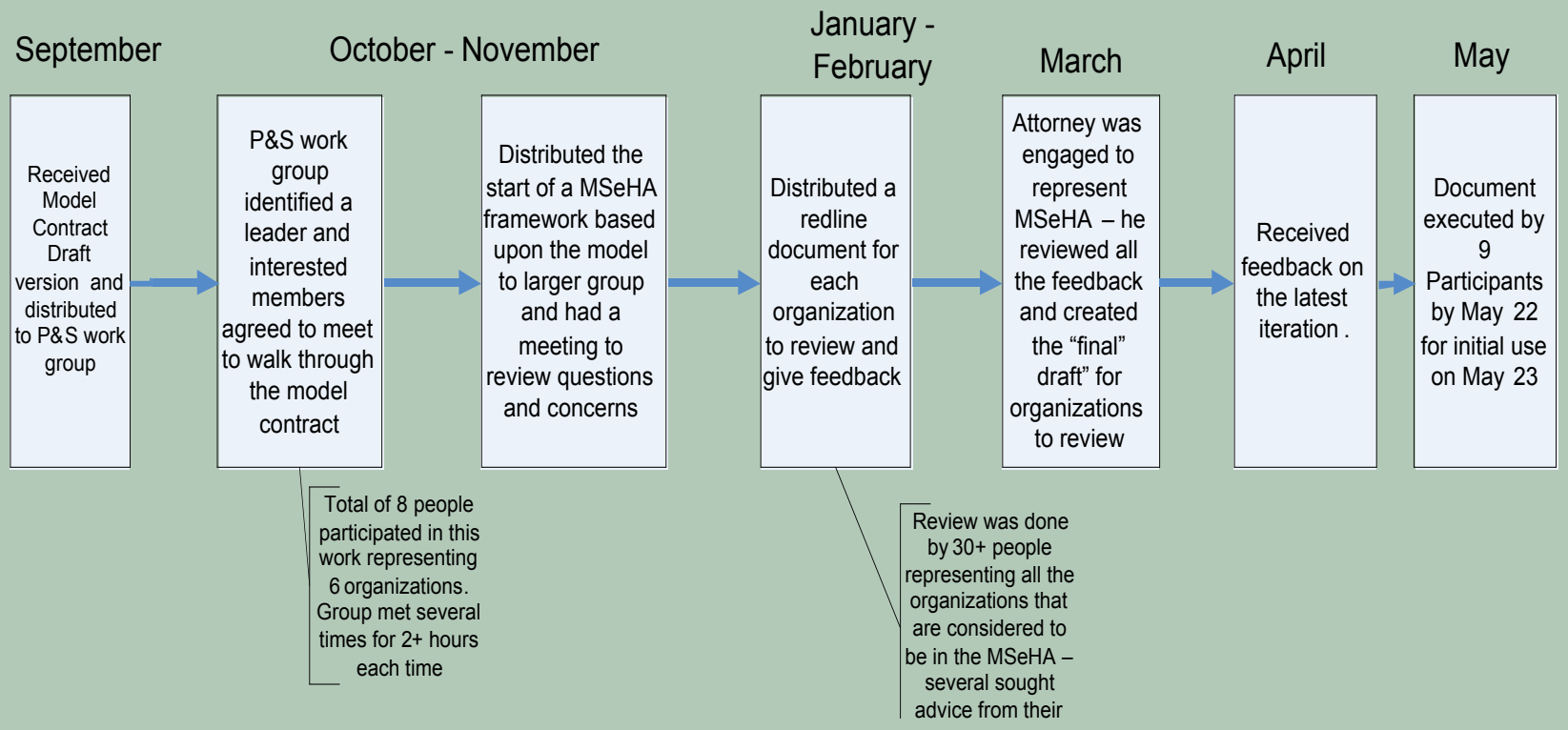
Project Overview

- Operational system managed through a new non-profit organization (MidSouth eHealth Alliance); 15 “publishers” and used now in emergency departments
- Comprehensive information – not just claims
- Members bound together by formal data-sharing and user agreements

Legal and Policy Framework

- Based on Connecting for Health (CFH) Principles
- Derived from CFH model contracts
- Development process
- Registration agreement
- Participation agreement
- User agreements
- Operations committee

Policy development takes time



Our overall approach was to do as much work as we possibly could without incurring legal fees

MSeHA = Mid-South eHealth Alliance P & S = Privacy and Security

Principles: Markle

- Openness and Transparency
- Accountability and oversight
- Data issues
  - Data integrity and quality
  - Purpose specification and minimization
  - Collection limitation
  - Use limitations
- Security safeguards and controls
- Individual participation and controls
- Remedies

Nine Domains / Themes (HHS / HISPC)

- Authentication
- Authorization
- Patient and provider identification across multiple sites
- Security of information transmission
- Protections to prevent modification
- Audits to record and monitor activity
- Administrative and physical security safeguards
- State law restrictions about information types and classes
- Information use and disclosure policies that arise when institutions share health care information

Source: **http://www.health.state.mn.us/e-health/mpsp/ninevardomains.pdf**

Policy: NCVHS, February 2006

- Rights, obligations, and potential liabilities of all stakeholders
- Consumers participation
- Security and confidentiality
- Exchange with EHR and other data sources

http://www.ncvhs.hhs.gov/0602nhiirpt.pdf

Security: NCVHS recommendations

- Terms and conditions of use
- Consumer control and restrict access
- Consumer control of partial access
- Consumer ability to audit access
- Industry- standard security and authentication schemes

http://www.ncvhs.hhs.gov/0602nhiirpt.pdf

What we think we have right in Memphis

- Transparent and open policies
- Board and operations committee oversight
- Data – use limitations; integrity; purpose specification
- Individuals can “opt out”
- Security practices in place – including very strong access controls and audits

What we wish we could do better in Memphis

- Understand the trade-offs; why are we so concerned if others are following simpler procedures? (e.g., name, password)
- Authentication – two-factor, but is this even enough?
- Authorization – based on location & role
- Identity management processes – how to scale and maintain them?

What we really don't know

- What trade-offs must we consider?
- Where does use of a PHR (or misuse) violate laws (e.g., HIPAA, G-L-B, FACTA) ?
- How much uniformity must there be?
  - Technical
  - Policy
  - Social
  - Clinical
- Who decides? The "market"? (what market?)
- What happens when things "break"?

Some trade-offs

- Individual preference vs. technical capability or administrative burden
- Rights of the individual vs. rights on the public / payer / or other agent
- Early “cementing” of definitions to reach consensus vs. a portfolio of initiatives that may be difficult to reconcile
- Power (capital, size) vs. autonomy

Lessons learned

- Leadership is essential; information is power; information is politics
- Portfolio of efforts with open learning
- Competition over the right things
- Change takes time; everybody gives
- Technology & policy are intertwined
- Patient confidentiality comes first
- Broad research agenda is essential


VOLUNTEER EHEALTH INITIATIVE
HOME
RESOURCES
CALENDAR
NEWS
AHRQ
ABOUT US
CONTACT US
MEMPHIS
Previous
The MidSouth eHealth Alliance Data Sharing Agreements and Supporting Documents
FORE / AHIMA Report
The Tennessee eHealth Advisory Council
Tennessee one of 9 States Participating in HHS / AHIMA Study
Governor Bredesen, Healthcare Leaders Launch Campaign to Help Thousands of Tennessee Physicians Start e-Prescribing
Volunteer eHealth Initiative Described in Recent AHRQ-funded Report
Technical Advisory Panel Member Featured in Wall Street Journal
Doctors Explore Prescription Usage
Harvard and Industry Partners Announce Open-Source, User-Centric Identity Management Project
CareSpark to co-Sponsor May 6 EMR Meeting
Tuesday, September 26, 2006
The MidSouth eHealth Alliance Data Sharing Agreements and Supporting Documents
As of September, 2005, the MidSouth eHealth Alliance (MSeHA) and the AHRQ/TN State regional demonstration project is receiving comprehensive clinical data (labs, reports, diagnoses, etc.) from 15 organizations and is in operation in several emergency departments in the greater Memphis Area.
Our work led us to conclude that data-sharing agreements are critical. This process was based on data-sharing and other documetns from the Markle Connecting for Health Policy Group. The process took much longer than expected but served as a vital means of bringing over 50 people within the region to a more common, patient-centered goal.
The MidSouth eHealth Alliance is a non-profit company chartered specifically to manage the data exchange demonstration project and is supported by multiple sub-groups and an inclusive operations committee working continually on updating policies and procedures.
We present on th
our work.
http://www.volunteer-ehealth.org

Connecting Americans to Their Health Care:
Empowered Consumers, Personal Health Records and Emerging Technologies

2006

Policies 101: Health Privacy Policy from the Consumer Perspective

Paul Feldman
Health Privacy Project

MARKLE FOUNDATION
Robert Wood Johnson Foundation

What Do Consumers Want?
Privacy

- "…the right to be let alone."
  Samuel Warren and Louis Brandeis, "*The Right to Privacy*" (1890)
- "… individuals need to determine for themselves when, how, and to what extent information about them is communicated to others."
  Alan Westin, *Privacy and Freedom* (1967)

What Do Consumers Want?
Benefits

- Improved quality
- Greater accountability
- More participation and better decision-making
- Share in cost savings
- Fewer errors
- Reduced duplication

What Do Consumers Want?
Firewalls

- Employer
- Insurers (life, disability)
- Mortgage banker, credit provider
- Idiosyncratic (parents, ex, ???)

What Do Consumers Want?
Limits on Uses and Disclosures

- **Granular**: Share this (longitudinal blood pressure) but not this (prior myocardial infarction):
  - Incredibly individual and unpredictable
  - Not just the likely suspects (HIV, substance abuse, mental health, reproductive and sexual health)
  - Genetic information coming your way

What Do Consumers Want?
Limits on Uses and Disclosures

- **Situational**
  - Who: Share heart attack history with her (cardiologist) and him (periodontist) but not her (neighbor who runs my dentist's front desk)
  - Why:
    - Share everything with my care providers and nothing with marketers
    - syndromic surveillance – yes or no?

What Do Consumers Want?
Consent and Notice

- Consent
  - Opt-in v. opt-out
  - Conditional?
- Notice
  - Meaningful, plain language

What Do Consumers Want?
Security

- The Las Vegas Doctrine: What happens in my nurse practitioner's office stays in my nurse practitioner's office!
- Anyone who holds PHI is expected to protect it and is accountable for its security.

What Protections do Consumers Have?

- HIPAA
  - Privacy Rule
  - Security Rule
- State laws and regs
- GLBA, FACTA, FTC, FERPA

HIPAA Reach

- Applies to Covered Entities (CE)
  - Healthcare providers
  - Health plans
  - Clearinghouses
- Business Associates (BA)
  - Where do RHIOs fit in?
- PHRs: Only if CE or BA of CE

Consumer Rights under HIPAA

- Receive notice of privacy practices
- See and copy own health information
- Expect security
- Request amendment
- Receive an accounting of disclosures
- Request restrictions
- Receive confidential communications

Duties of Covered Entities

- Comply with restrictions on use and disclosure of protected health information (Privacy Rule)
  - IIHI, de-identified HI, aggregated HI
  - Restrict information disclosed to minimum amount necessary to accomplish the purpose.
  - More permissive for TPO
- Secure PHI (Security Rule)

Consumer Protections for PHRs

- Privacy and Security Rules apply if PHR provider is a CE or BA
- FTC requires seller to adhere to stated (privacy) policies, but doesn't require existence of policies
- State laws

Enforcement

- OCR charged with enforcing Privacy Rule and CMS with Security Rule
- Voluntary compliance
- Civil Monetary Penalties
- Referral to Department of Justice for criminal prosecution
- States

Consumer Health Privacy Hot Buttons

- Preemption of state laws/regs
- Adherence to “minimum necessary”
- Medical identity theft
- Breach notification
- Secondary uses
- Genetic information
- Disclosure across firewalls (employers, insurers)

Needed Fixes

- PHRs regulation, regardless of provenance
- Meaningful enforcement of HIPAA and PHRs, with penalties and criminal convictions
  - Include employees, not just CEs
- Plain language, meaningful Notice of Privacy Rights

More Fixes

- Provoke a shared expectation of “policy baked into technology”
  - End promulgating technology standards without policy principles in place
- Private right of action (remedy)
- Breach notification
- Regulation of RHIOs

Keep in Mind

- Encourage participation in population health activities
  - natural history studies
  - public health event alert
- Encourage participation in research
- Quality, quality, quality

For More Information

Paul Feldman
pfeldman@healthprivacy.org
www.healthprivacy.org

Connecting Americans to Their Health Care:

Empowered Consumers, Personal Health Records and Emerging Technologies

NATIONAL CONFERENCE
DECEMBER 7-8, 2006
WASHINGTON, D.C.