CONNECTING FOR HEALTH
COMMON FRAMEWORK

Resources for Implementing Private and Secure Health Information Exchange

Policies for Information Sharing

April 10, 2006

Mark Frisse, MD, MBA, MSc
Marcy Wilder, JD
Janlori Goldman, JD
Joseph Heyman, MD

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

- Work 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

- Some of the most challenging aspects of electronic health information exchange are "policy" related.
  - 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?

Connecting for Health Goals

- Develop a policy framework that enables information sharing to happen for high quality patient care while still protecting the privacy and security of personal health information.
- Identify what needs to be common for interoperability and what does not.
- Design and develop a working guide for the use of communities on issues such as access, control, privacy and security.

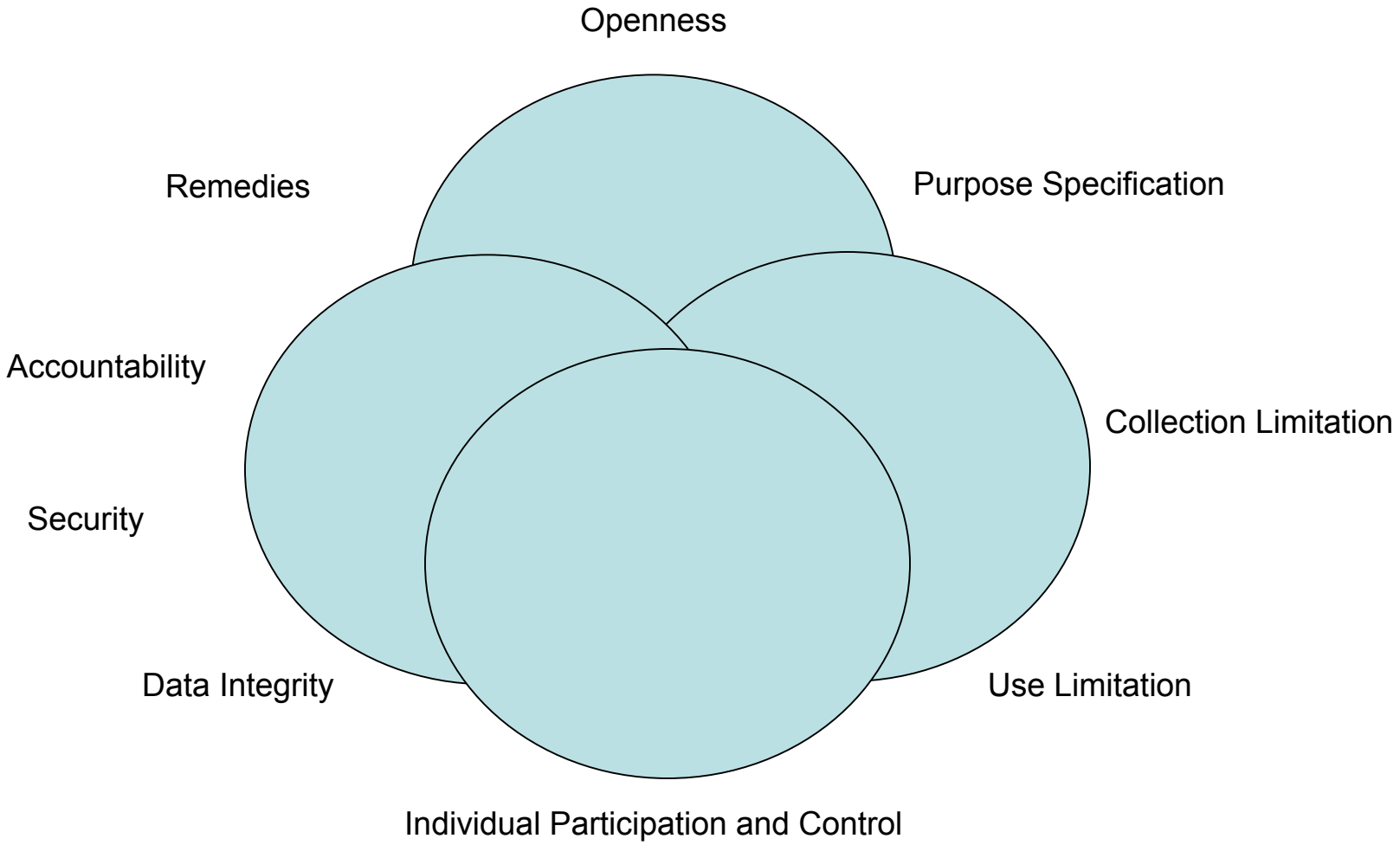
What is the Common Framework?

A secure nationwide health information exchange network will be enabled by the general adoption of a set of specific, critical tools, including technical standards for exchanging clinical information, explicit policies for how information is handled, and uniform methods for linking information accurately and securely.

Privacy in Networked Environments

- In a networked environment: persistent and aggregated “data shadow”
- Increased **risks** of misuse and re-use; not dealt with through consent
- Privacy protective behavior: opt-out of the system
- Demands a systemic privacy protection architecture (fair information practices) to mitigate the risks and establish trust

Connecting for Health Architecture for Privacy in a Networked Health Information Environment



P2: Model Privacy Policies and Procedures

- Establish baseline privacy protections – participants can follow more protective practices
- Based on HIPAA, although some policies offer greater privacy protections
- Rooted in nine privacy principles
- To be used in conjunction with *M2: A Model Contract for Health Information Exchange*

P2: Model Privacy Policies and Procedures

- SNO Policy 100: Compliance with Law and Policy
- SNO Policy 200: Notice of Privacy Practices
  - Exceeds HIPAA requirements -- requires disclosure of information related to the SNO and RLS
  - Notice should inform individuals about what information may be available through SNO and RLS, who can access it, and to have information about them removed from the RLS

P2: Model Privacy Policies and Procedures

- SNO Policy 300: Individual Participation and Control of Information Posted to the RLS
  - Exceeds HIPAA requirements by allowing individuals to decide whether or not to have information included in RLS
  - Coverage or care cannot be withheld on the basis of the individual's choice

P2: Model Privacy Policies and Procedures

- SNO Policy 400: Uses and Disclosures of Health Information
  - Integrates HIPAA permissible purpose and minimization premises
  - Uses for TPO are permissible
  - Generally, uses for law enforcement, disaster relief, research, and public health are permissible
  - Marketing not permissible
  - Discrimination not permissible

P2: Model Privacy Policies and Procedures

- SNO Policy 500: Information Subject to Special Protection
- SNO Policy 600: Minimum Necessary
- SNO Policy 700: Workforce, Agents, and Contractors
- SNO Policy 800: Amendment of Data
- SNO Policy 900: Requests for Restrictions

P3: Notification and Consent When Using a Record Locator Service

- Addresses question: what should an institution participating in the RLS be required to do to inform patients and give them the ability to decide not to be listed in the RLS index?
- Recommendation more protective of privacy than HIPAA

P3: Notification and Consent When Using a Record Locator Service

- Information on patients of participating institutions included in RLS on day one (patient names, demographics, and institution names)
- Patient must be given notice that institution participates in RLS and provided with opportunity to opt-out of index
- Revision of HIPAA Notice of Privacy Practices
- Initial Inquiry Audit
- Patient access to RLS record

P8: Breaches of Confidential Health Information

- SNO will comply with HIPAA Security Rule. SNO Participants will comply with applicable federal, state, and local laws
- Responsibility of Participants to train personnel and enforce institutional confidentiality policies and disciplinary procedures

P8: Breaches of Confidential Health Information

- SNO must report any breaches and/or security incidents. SNO Participants must inform SNO of serious breaches of confidentiality
- Participants and SNOs should work towards system that ensures affected patients are notified in the event of a breach

P8: Breaches of Confidential Health Information

- SNO contract could include provision allowing Participant withdrawal from SNO in case of serious breach of patient data
- SNO contract could include indemnification provisions pertaining to breach of confidentiality of protected health information

P6: Patients' Access to Their Own Health Information

- HIPAA
  - Right to See, Copy, and Amend own health information
  - Accounting for Disclosures
  - Covered entities required to follow both Privacy Rule and related state laws
  - Allows stronger privacy safeguards at state level

P6: Patients' Access to Their Own Health Information

- Patient access to the information in the RLS
  - Each SNO should have a formal process through which information in the RLS can be requested by a patient or on a patient's behalf
  - Participants and SNOs shall consider and work towards providing patients direct, secure access to the information about them in the RLS