

CONNECTING FOR HEALTH COMMON FRAMEWORK

Resources for Implementing Private and
Secure Health Information Exchange

Methods for Achieving Information Exchange (July 18, 2006 - Cambridge, MA)

Bill Braithwaite, MD, PhD
eHealth Initiative

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.

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 information exchange 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 privacy and security protections?
 - Who shares what and who bears the liability?
 - How can you control access to your information?

What is the Common Framework?

Secure nationwide health information exchange 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.

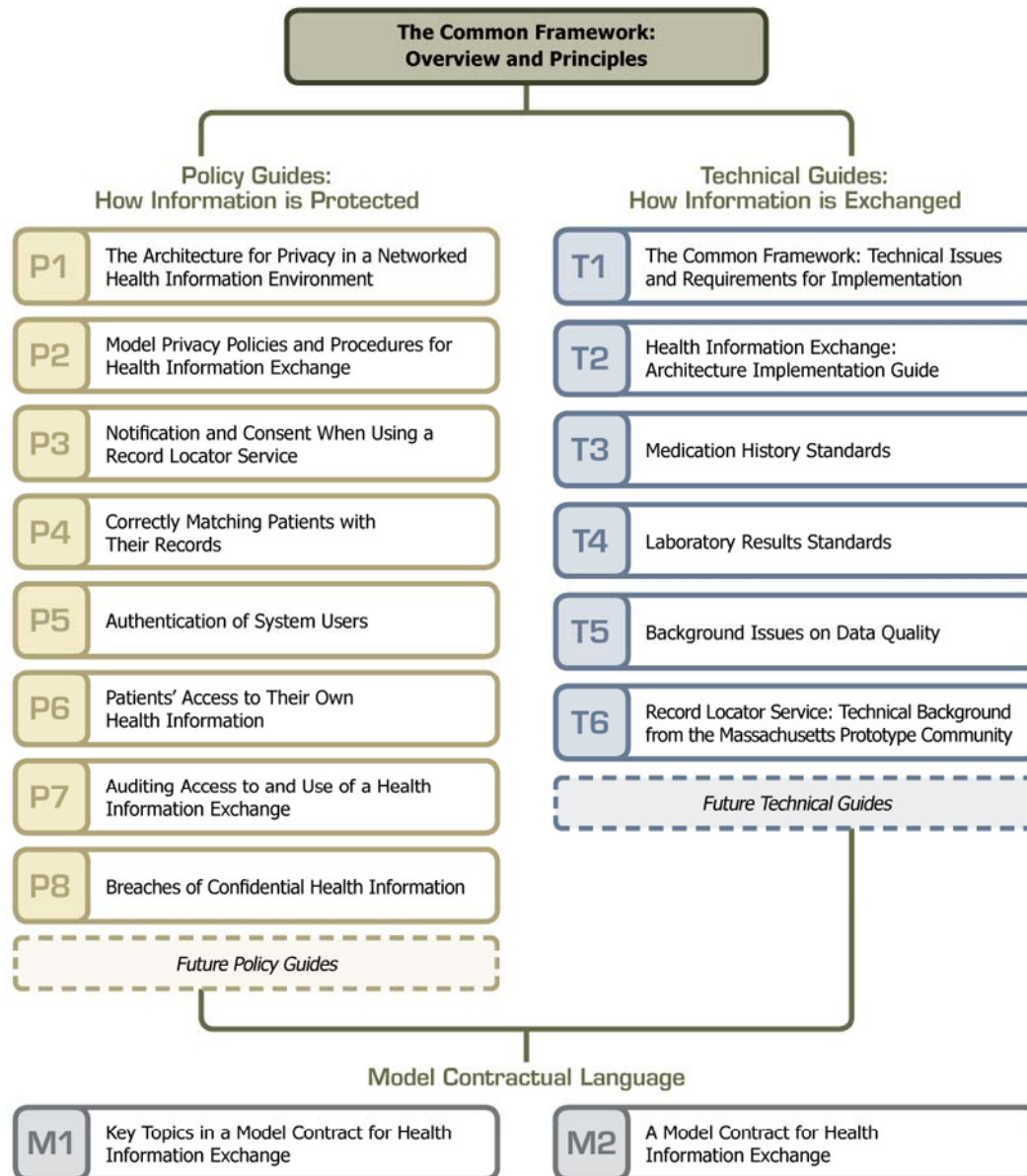
Overview of Connecting for Health Architecture

A sub-network organization (SNO) brings together a number of providers and other health information sources:

- 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



P4: Correctly Matching Patients with Their Records

- Record Locator Service (RLS)
 - Participating entities control whether or not to publish record locations to RLS
 - Queries only by authorized participants
 - Contains no clinical information
 - Designed to take a query in the form of demographic details and return only the location of matching records
- Obtaining the actual clinical record is a separate transaction NOT involving the RLS.

P4: Correctly Matching Patients with Their Records

Challenge: How to optimize matching probabilities while minimizing incidental disclosures caused by false positive matches within the Record Locator Service?

Recommendation: Utilize a probabilistic matching algorithm with a high probability threshold for matching.

P4: Correctly Matching Patients with Their Records

- A false positive match is an “incidental disclosure” under HIPAA
- What should we recommend to minimize such disclosures?
 - A minimal level of certainty of 1 in 100,000 before the RLS returns a matching record
 - No “wild-card” queries
 - Return no data not contained in query
 - No “Break the Glass” queries

P4: Correctly Matching Patients with Their Records

- What should we recommend for actions to take when such disclosures occur?
 - Immediate destruction of information received from the RLS that does not apply to the patient at issue
 - No need to report

P4: Other RLS Functions

- Each SNO is free to develop greater functionality
- Error checking is highly recommended
 - Data field edits when records published
 - Possible Type 1 and Type 2 errors made by publishing entity
- Optional subscription services
- Access reports

P5: Authentication of System Users

- Identity (Who am I?)
- Identifiers (How is that Identity represented?)
- Authentication (How can I prove who I am?)
- Authorization (What can I do when I've proved who I am?)

P5: Authentication of System Users

- Requirements
 - Transitive trust, often based in contract
 - SNO must have identifiers for all participating entities
 - Users must be authenticated before given access to any SNO-wide resource containing patient data
 - Any request for data from a remote institution must have two pieces of identifying information (institution authenticating user and identifier for user)

P5: Authentication of System Users

- Requirements
 - “Break the Glass” function may be allowed (although not allowed in RLS itself)
 - Must be accompanied by description of rationale for request
 - Must be accompanied by an identifier for the user.
 - No “Emergency” account (role without identifier)
 - Requires timely human review and enhanced auditing

P5: Authentication of System Users

- Requirements
 - For patient to access his or her own records, initial access must be provided by participating institution or third-party recognized by SNO

P7: Auditing Access to and Use of a Health Information Exchange

- HIPAA
 - Privacy Rule does not specifically mention audits or logging but requires covered entities to have in place appropriate safeguards
 - Security Rule requires audit controls as a standard
- State laws may also exist

P7: Auditing Access to and Use of a Health Information Exchange

- Recommendations:
 - Participants within the SNO would follow baseline audit and logging requirements of HIPAA Security Rule
 - Varies with the Security Environment (“scalable”)

P7: Auditing Access to and Use of a Health Information Exchange

- Recommendations
 - SNO itself expected to be sophisticated entity, operating at a scale consistent with rigorous audit and other security practices.
 - Likely to rely more heavily on electronic health records in near term

P7: Auditing Access to and Use of a Health Information Exchange

- Recommendations
 - RLS should follow strong logging and audit control standards, applied with transparent and effective methods
 - RLS structure means that flow of demographic information will be carefully tracked at RLS level
 - Transfers of clinical records will not take place through RLS; will be subject to logging and audit practices of each entity

P7: Auditing Access to and Use of a Health Information Exchange

- Additional logging and audit control functions recommended at SNO and RLS levels
 - Audit of VIP records
 - Procedures for follow-up on suspicious activity, such as indications of possible breaches
 - Review of network intrusion detection system activity logs
 - Review of physical access to data centers
 - Other review of technical, physical, and administrative safeguards
 - Random audits of demographic and clinical records, based on the level of risk for that portion of the system.

Questions?

Bill.Braithwaite@eHealthInitiative.org