eHI Toolkit for Health Information Exchange

Building and Maintaining Policies for Information Sharing

Bill Braithwaite, MD, PhD

eHealth Initiative

eHEALTH INITIATIVE
Real Solutions, Better Health

http://toolkit.ehealthinitiative.org/

Common Principles and Policies for Information Sharing

- HIE requires trusted relationships
  - or data sources will not be willing to share the data they hold.
- Each participant in HIE must agree to follow certain information sharing policies and procedures.
  - agreement must be under contract.
  - must be minimum necessary and not impinge on local decisions unless absolutely necessary.
  - all agreement terms must be based on mutually agreed upon principles.

Privacy and Security

- Two of the most difficult areas are privacy and security.
- Reasons: misunderstanding, unfounded apprehension, or specific fears.
- ‘Privacy’ is also blamed when other causes are at work.
  - e.g., lack of trust or competitive instincts.
- All parties must learn about and understand underlying principles on which trust and consensus may be built.
- Experience of existing HIE efforts shows that this is an interactive process that cannot be rushed.
- Most efforts start off with something that everyone feels comfortable with;
  - typically the sharing of health information between healthcare providers for treatment purposes.

Adding Use Cases

- Adding use cases makes interactions between principles and applicable policies and procedures more difficult and consensus less easy to achieve.
- Example: biosurveillance for public health purposes brings up questions that require agreement:
  - What data sources report what data in what time frame?
  - What are the legal and ethical drivers to report this data?
  - What protections do the data have once received by public health?
  - Can patients opt-out from this type of reporting, and if so, how?
  - Are the data reported in identified or de-identified form?
  - If de-identified, what policies and procedures allow for re-identification for specific investigations, and by whom?

Who gets to participate in the HIE?

- Example: clinical data held and processed electronically for claims purposes by health plans and their agents (e.g., pharmacy benefit managers or PBMs) could be very useful in clinical situations where the original data is unavailable electronically.
  - If the HIE project allows health plans to share such data, are they also allowed to search for other clinical data on their beneficiaries, and for what purposes?
  - In addition to the practical issue about whether other clinical data sources will agree to be part of the system under such circumstances, particular privacy and security issues arise:
    - How are patients notified of the potential disclosure of their information to their payers?
    - How will patients be given control over such disclosures or must they opt out of the whole system?
    - How does one define and control the purpose for which information is being sought?
    - How are the roles of authorized users defined and controlled and to what information can they have access under what circumstances?

Technical Relationship to Policy

- Technical and architectural decisions also affect what privacy and security policies and procedures must be defined.
- If a record locator service is used to locate sources of data, are the privacy and security policies and procedures different from those used for direct queries for the clinical data, and how?
- If clinical data are to be copied and standardized in preparation for responding to a query, how is the control of the data steward maintained over the copies and implemented in the resulting proxy server?

Cultural Context

- The cultural context of the HIE effort can also make a difference:
  - In some regions, an HIE can declare a policy that all clinical information will be available for sharing, with appropriate controls and constraints, and that patients may not opt out (they must go elsewhere for their healthcare if they don't want to participate).
  - In other regions, the local culture would require more patient control and ability to opt out of participation in the data sharing system.
- How do you get community consensus on a particular approach?

Privacy Principles

Earliest public documentation of concept of "Fair Information Practices Principles“ was the 1973 "Richardson Report" on "Records, Computers and the Rights of Citizens".

1. **Notice**: Data collectors must disclose their data collection.
2. **Choice**: Data subjects should have rights to opt out of uses and disclosures of their data.
3. **Access**: Data subjects should be able to view their information and have it corrected if necessary.
4. **Security**: Data collectors must take reasonable steps to ensure that their data is accurate and protected against unauthorized use and disclosure.

First codified in law in the Privacy Act of 1974

- applicable only to federal agencies, and have been the model for most privacy laws ever since, including HIPAA.

5 Common Principles of Fair Information Practices

- **Notice**
  - The existence and purpose of record-keeping systems must be known to the individuals whose data is contained therein.
- **Choice**
  - Information must be collected only with the knowledge and implicit or explicit permission of the subject, used only in ways relevant to the purpose for which the data was collected, and disclosed only with permission of the subject or in accordance with overriding legal authority (such as a public health law that requires reporting of a serious contagious disease).
- **Access**
  - Individuals must have the right to see records of information about them and to assure the quality of that information (accuracy, completeness, and timeliness). In healthcare, records are rarely deleted or replaced, but this principle implies that there is at least a due process for individuals to amend poor quality information about them.
- **Security**
  - Reasonable safeguards must be in place for the confidentiality, integrity, and availability of information.
- **Enforcement**
  - Violations must result in reasonable and consistently applied penalties to deter violators and in reasonable mitigation efforts to offset the effects of a breach as much as possible.

Context of Privacy Principles in HIE

- It is important to adopt such a set of principles and constantly refer back to them when making decisions about health information sharing policies and procedures.
- Everyone involved must buy into the principles you choose to work with and be thoroughly familiar with them, their effect on the agreements that must be made, and the consensus that must be reached before a community is able to implement health information exchange.

Security Principles

- You cannot have privacy (or confidentiality of private information) without security measures to protect the information from being used or disclosed in ways that violate the other principles.
- Information must be available and, to be trusted, it must have integrity such that it cannot have been altered between the data source and the decision maker.
  - These characteristics of confidentiality, integrity, and availability are the backbone of health information security.
- To support all three, security must be implemented as a careful balance of administrative, technical, and physical safeguards which are tailored to the particular information systems environment of each installation.

Recommended Approach

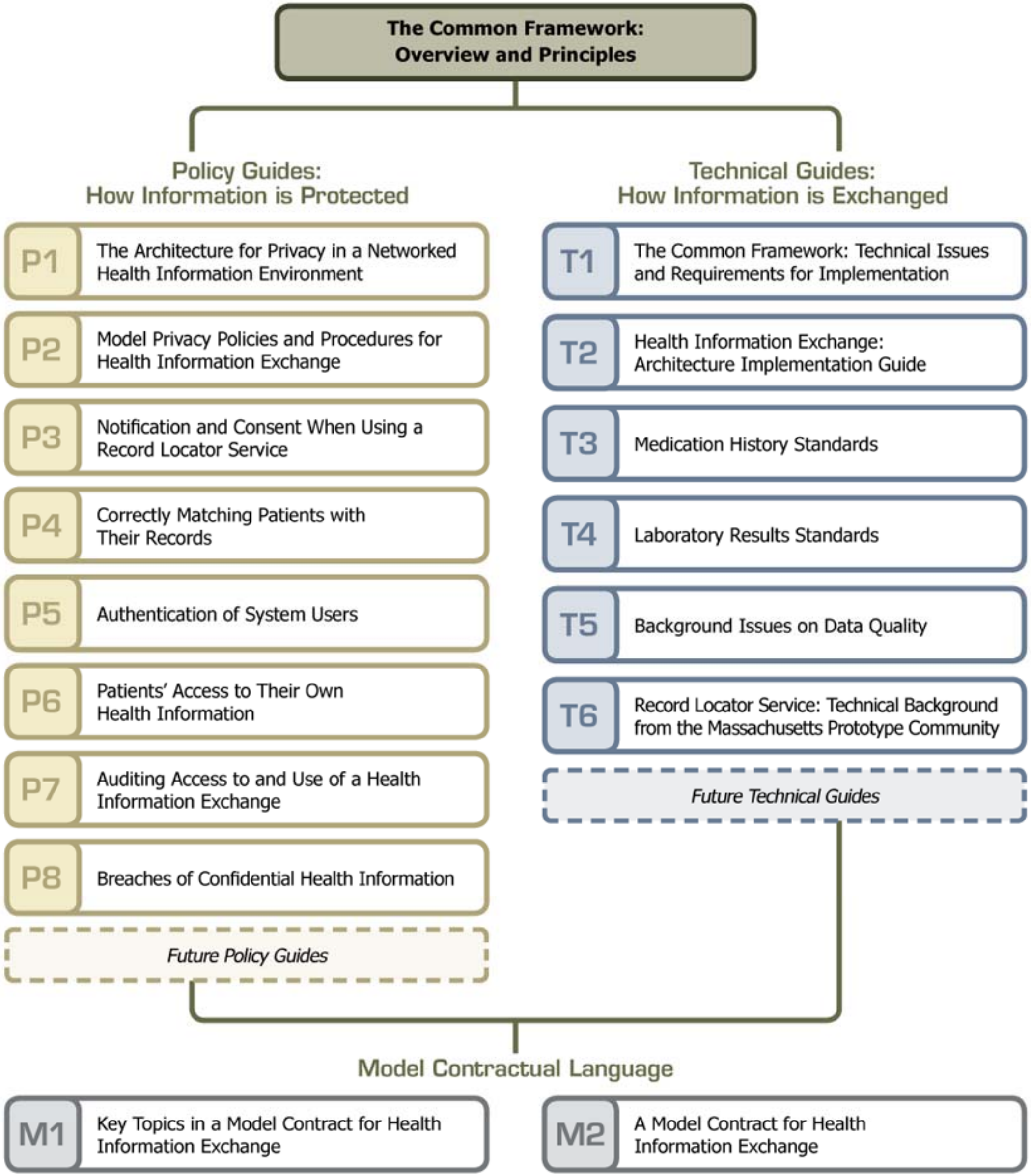
- Risk assessment of the information systems environment followed by
  - ongoing risk management through the selection, implementation, and monitoring of reasonable and appropriate measures to minimize the risks while controlling the costs.
- This flexible and scalable approach is the basis for the HIPAA security rule, taken because security threats and solutions evolve too quickly to be writ in stone (as it were) in the form of federal regulation.
  - Often, these measures involve policies, procedures, and contracts with business associates more than technology.
- The majority of security breaches are from the ‘inside’, and for security technology to work, behavioral safeguards must be established and enforced.
  - This requires administrative commitment and responsibility at the highest executive level in an organization.

Security for HIE

- The HIPAA rule provides good general guidelines to follow for health information security.
- In general, particular attention must be paid to the following areas of security when designing the policies, procedures, and agreements for HIE:
  - User identification and authentication
  - User authorization
  - Role based access control
  - Transmission security
  - Minimum necessary
  - Audit trail and information system activity review
  - Response to security incidents including reporting, sanctions, and mitigation

Organizational Challenge: Multi-level, Multi-stakeholder, Multi-institution, Multi-Lateral Agreements

- Outside the purely technical realm, the most difficult problems involve getting consensus or agreement across all the institutions that propose to exchange health information.
- They all have to agree at the high level principles level, at the nationwide policies and procedures level, and at the local, regional level of implementation.
- All these levels of agreement must be committed to in contract language, a model for which is found in the toolkit.



The Common Framework: Overview and Principles

Policy Guides: How Information is Protected

- P1 The Architecture for Privacy in a Networked Health Information Environment
- P2 Model Privacy Policies and Procedures for Health Information Exchange
- P3 Notification and Consent When Using a Record Locator Service
- P4 Correctly Matching Patients with Their Records
- P5 Authentication of System Users
- P6 Patients' Access to Their Own Health Information
- P7 Auditing Access to and Use of a Health Information Exchange
- P8 Breaches of Confidential Health Information
- *Future Policy Guides*

Technical Guides: How Information is Exchanged

- T1 The Common Framework: Technical Issues and Requirements for Implementation
- T2 Health Information Exchange: Architecture Implementation Guide
- T3 Medication History Standards
- T4 Laboratory Results Standards
- T5 Background Issues on Data Quality
- T6 Record Locator Service: Technical Background from the Massachusetts Prototype Community
- *Future Technical Guides*

Model Contractual Language

- M1 Key Topics in a Model Contract for Health Information Exchange
- M2 A Model Contract for Health Information Exchange

Model Privacy Policies and Procedures

- To be used in conjunction with the *Model Contract for Health Information Exchange*
- 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
- Should be customized to reflect participants' circumstances and state laws

Model Contract for Health Information Exchange

- Purpose of Model SNO Terms and Conditions
  - To assist SNOs prepare their own Terms and Conditions
  - 60-40 solution
  - Identify issues and alternatives
  - Raise questions

Model Contract: Essential Components

- Incorporates applicable terms of Common Framework Policies and Procedures
- Provides specific terms that the individual SNO may determine are appropriate for its unique needs
- Includes mechanism for making and implementing changes

eHEALTH INITIATIVE
Real Solutions, Better Health

Common Framework
Policy Topics Addressed

- Notification and consent
- Uses and disclosures of health information
- Matching patients with their records
- Authentication
- Patient access to their own information
- Audit
- Breaches of confidential information

What is Available?

Policy Documents: 3 Categories

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

Common Framework Resources

- All available free at a link from the eHI Toolkit or 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

Performance Measurement Principles

- Principles derived from the long-term perspective that any quantitative or qualitative evaluation of the performance of clinicians should be based on information that is, or should be, available to the clinician when making clinical decisions.
- Only when the information is brought into the clinician's EHR and made available to the CDSS in computable form can we expect the clinician's performance to reach the highest quality.
- The following common principles have been vetted with the AMA and NCQA and are under consideration by the AQA.

Performance Measurement Principles

- Transmitting data to quality measurement programs should not be stand-alone but should use the same message standards as other efforts to interoperate between clinical systems (e.g., lab transmits results to ambulatory EHR system).
  - The implementation guide provided by DOQ-IT is a non-standard HL7 implementation using ‘Z’ segments and would not be used in other interactions with an EHR system.
  - Quality programs should use the same security and transmission infrastructure as other efforts to interoperate with EHR systems (e.g., transmission media, encryption mechanisms, authentication methods, etc.).
- Quality measures should be based on data that is found (or should be found) in the EHR system for clinical purposes and not require special data entry (e.g., use value of LDL-C, not a check box indicating LDL-C is above 200).
  - If clinical data is judged to be appropriate for a quality measure but is not found in an EHR system, it should be evaluated to see if it should be added to the EHR system for appropriate documentation for clinical purposes.

Performance Measurement Principles

- Quality programs should try to generate quality reports from de-identified patient data to protect patients' privacy and guard against identity theft.
  - The alternative of a limited data set under a data use agreement should be considered only if the program cannot be conducted with de-identified data.
- Quality measures should use data that is not required to be removed in de-identified data whenever possible (e.g., use 'age' instead of subtracting birth date from visit date).
- Quality measures should specify code sets appropriate for EHR systems (e.g., NDC codes are found in pharmacies but not in EHR systems; RxNorm is a more appropriate code system for drugs in EHR systems).

Performance Measurement Principles

- Quality measures should include criteria at the clinical level of detail with the expectation that EHR systems will record it for clinical purposes (e.g., include SNOMED codes as well as CPT and ICD codes in selection criteria; SNOMED can be mapped to ICD for billing purposes).
- Quality measures should use negatives carefully in context (e.g., patient reason for refusing the attempt to prescribe an indicated drug is difficult to record, retrieve, and transmit in standard ways).
- Quality measures should use verbs carefully so that criteria are likely to be recorded in the EHR system (e.g., a drug can be prescribed, administered, taken, filled, refilled, distributed, refused, etc.; but only 'prescribed' is likely to be recorded consistently in EHR systems at this time).

Questions?

Bill.Braithwaite@eHealthInitiative.org