HIPAA Summit XII

Role of HIPAA Compliance in HIT Initiatives

Bill Braithwaite, MD, PhD

eHealth Initiative

April 11, 2006

eHEALTH INITIATIVE
Real Solutions, Better Health

http://toolkit.ehealthinitiative.org/

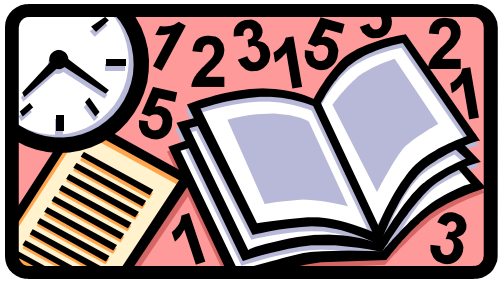
eHI is the "Go-to" Organization for State and Regional HIT and Health Information Exchange Efforts

Advocacy

eHealth Initiative and Foundation

Grants

Hands-on Help



Knowledge

eHI Toolkit for Health Information Exchange

eHEALTH INITIATIVE
Connecting Communities Toolkit

Comprehensive on-line, interactive resource that walks the community through the seven critical components of success:

- Getting started: Assessing environment, engaging stakeholders, developing shared vision and goals
- Organization and governance, legal issues
- Value creation, financing and sustainability
- Policies for information sharing
- Practice transformation and quality improvement
- Technical implementation
- Public policy and advocacy

eHI's Connecting Communities Toolkit- *Launched Jan 31, 2006*

eHealthIntitative - Toolkits - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://toolkit.ehealthinitiative.org/ Go Links

Google Norton Internet Security Norton AntiVirus

DevToolBar View DOM Disable View Outline Validate Images Resize Misc Show Ruler

eHI Home Page • Toolkit Home • Connecting Communities Members • Contact Us • Sitemap

eHEALTH INITIATIVE
Connecting Communities Toolkit

Getting Started | Organization and Governance | Value Creation and Financing | Practice Transformation | Policies for Information Sharing | Technology | Public Policy and Advocacy

First time to this website? CLICK HERE to Gain Access Through FREE Registration

eHealth Initiative's Third Annual Connecting Communities for Better Health Learning Forum April 9th - 11th , 2006 Washington, D.C. more...

What is Health Information Exchange? Learn more by Downloading the Second Annual Survey Of State, Regional And Community-Based Health Information Initiatives And Organizations more...

Key Findings from the 2005 eHI Annual Survey of Health Information Exchange more...

Welcome to the eHealth Initiative's Connecting Communities Toolkit

Communities across the country are mobilizing information across organizations through multi-stakeholder collaboratives made up of a broad range of constituencies. The *Connecting Communities Toolkit* supports learning across and among diverse stakeholders including state, regional and community-based organizations. The majority of the information in the *Toolkit* is available **free of charge** to the general public

The *Toolkit* is a distillation of the knowledge that the eHealth Initiative has accumulated through its work with multiple stakeholders and different communities. Stakeholders from every sector of healthcare, pioneers who are mobilizing information at the state, regional and community levels, and leading experts have provided significant input into a set of common principles and guides in seven *Toolkit* modules, each including easily accessible online documents and tools. Now, states, regions or communities can use one or more modules to move forward with confidence and at a more rapid pace.

Each *Toolkit* module includes an introduction and overview, a roadmap, key principles, sample community experiences, and a set of resources and links specific to the module, all of which are available to the publicfree of charge. (CLICK HERE TO REGISTER FOR FREE AND GAIN ACCESS TO THE TOOLKIT.) Much of this work was supported by funds from a cooperative agreement of the Health Resources Services Administration Office of the Advancement of Telehealth.

The *Toolkit* is divided into seven distinct modules:

Search Go

Connect with Communities
Our Partners
News and Events
Glossary
Provide Feedback
Register

Internet

Module Components

- Each module is composed of:
  - Introduction and overview
  - Common Principles
  - Roadmap
  - Community Experiences
  - Tools
  - Resources
  - Leadership
  - Glossary
  - Feedback

Common Principles and Policies for Information Sharing (e.g.)

- 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 should be under contract.
  - should be minimum necessary and not impinge on local decisions unless absolutely necessary.
  - all agreement terms should 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". http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm

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.

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.

HIPAA v. Privacy State Law

- Privacy: HIPAA supersedes contrary state law except when more stringent.
  - State law is hard to find – elements of statute, regulation, and case law are scattered and issue specific.
  - Some states are passing new law – some deals with perceived gaps in HIPAA.
  - Integrating HIPAA with state law across multiple state is very difficult (and expensive).

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.
- The most confidential information is that which is secured in such a way that no one but the originator can access it.
  - that is inappropriate in the field of healthcare where the purpose of such information is to be available when and where needed to improve clinical decision making about the subject whenever and wherever the subject appears for healthcare.
- To be trusted, information 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

- This is best done through a 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 administration commitment and responsibility at the highest executive level in an organization, without which any security measure is likely to fail.

Nut Shell

- In a nut shell, security involves the documentation of the implementation of reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of electronic health information.
- Since security is such an important and visible aspect of HIE programs, it is important to identify and make known the person responsible for the development and implementation of the policies and procedures as well as the implementation and ongoing maintenance of security measures for the HIE.
- The HIPAA rule provides good general guidelines to follow for health information security, but there are a few areas that should be emphasized for HIE projects which may be different based on the goal and implementation technology of the project.
- For example, if the HIE is simply to serve as a conduit between participants without access to the content, then the security aspects are much simpler than if the HIE is holding copies of the clinical data and responding to queries on behalf of the data sources.

Security for HIE

- 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

Privacy and Security Solutions

- An $11.5 million contract was awarded to the Health Information Security and Privacy Collaboration (HISPC), which is overseen by RTI International, a private, nonprofit organization.
  - The Collaboration will be working with state and territorial governments to assess and develop plans to address variations in organization-level business policies and state laws that affect privacy and security practices that may pose challenges to interoperable health information exchange.
  - The Agency for Healthcare Research and Quality (AHRQ) is participating in this initiative as well.

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.

HIPAA Business Associate Agreements

- Extend requirements beyond Covered Entities and set ground work for HIE agreements.
- Most HIE startup time spent on Privacy and Security policies and procedures and on getting consensus (signed contracts) to follow them.

Markle Foundation Connecting for Health project

- To 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.
  - Understand what needs to be common for interoperability and what does not.
- The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange
  - Backgrounders, Model Policies, and a Model Contract.
  - Will be added to the eHI toolkit next week.

NHIN Policies and Procedures

- The NHIN Policies and Procedures will describe the terms and conditions that apply throughout the NHIN to all RHIOs and Participants.
- Standard terms govern how the NHIN will function, and the basic standards that will govern the operations of each RHIO, including implementation policies and procedures such as:
  - Privacy Policies;
  - Authorization and control, consent agreements;
  - Accurate patient identification;
  - Professional and institutional authentication;
  - Individual (patient/consumer/caregiver) authentication;
  - Security Policies (authentication, encryption, electronic signatures);
  - Interoperability user agreements;
  - Message transport standards;
  - Privacy and Security Practices; and
  - Data standards for priority use cases.
- In order to participate in the NHIN, each RHIO and their Participants will agree to abide by all the applicable terms of the NHIN Policies and Procedures.

Bill Braithwaite, MD, PhD
Chief Medical Officer
eHealth Initiative and Foundation

toolkit.ehealthinitiative.org
818 Connecticut Ave. NW Suite 500
Washington, D.C. 20006
202.624.3270
bill.braithwaite@ehealthinitiative.org