MIT HIT Symposium

How HIPAA Applies to HIT

Bill Braithwaite, MD, PhD
eHealth Initiative

eHEALTH INITIATIVE
Real Solutions, Better Health

Cambridge, MA July 17, 2006

A HIPPO on the Road to RHIO?

- There's got to be a Network in every Regional Health Information (Network) Organization!
- RHINO talking to RHINO makes the NHIN?
- HIPAA is still alive!

HIPAA Administrative Simplification

Sets standards for:

- Certain administrative transactions
- Code sets for concepts in transactions (ICD, CPT)
- Identifiers for providers, employers, plans, [patients]
- Privacy
- Security
- Enforcement

Applicability to HIT & (clinical) HIE

- Transactions are different; HIPAA doesn't apply.
- Some code sets are the same; most are not.
- Identifiers are the same; may not be complete.
- Privacy applies directly; may need interpretation to cover unforeseen situations.
- Security applies directly; no privacy without.
- Enforcement applies where other standards apply.
- Secretary of HHS could use power under HIPAA to adopt HIE standards, but has said he wants to use 'market forces' of the government.

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 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.
  - 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 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?

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.

5 Principles of Fair Information Practices

- Notice
  - Existence and purpose of record-keeping systems must be known.
- Choice – information is:
  - Collected only with knowledge and permission of subject.
  - Used only in ways relevant to the purpose for which the data was collected.
  - Disclosed only with permission or overriding legal authority.
- Access
  - Individual right to see records and assure quality of information.
    - Accurate, complete, and timely.
- Security
  - Reasonable safeguards for confidentiality, integrity, and availability of information.
- Enforcement
  - Violations result in reasonable penalties and mitigation.

Security Principles

- The most confidential information is that which is secured in such a way that no one but the originator can access it.
  - in healthcare, information must be available when and where needed 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.

Security 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.

Security 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.
- 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

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.

NHIN Policies and Procedures

- Standard terms governing 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.

BE REASONABLE!

- 265 times in final privacy rule.
- 72 time in final security rule.

Bill.Braithwaite@eHealthInitiative.org

eHEALTH INITIATIVE
Real Solutions, Better Health