Privacy and Security Solutions For Interoperable Health Information Exchange

Presented by
Linda Dimitropoulos, PhD
RTI International

Presented at
NCVHS Standards and Security Subcommittee • May 1, 2007

RTI INTERNATIONAL
3040 Cornwallis Road ■ P.O. Box 12194 ■ Research Triangle Park, NC 27709
Phone 312-456-5246 Fax 312-456-5250 E-mail lld@rti.org

Overview

- Brief overview and current status update
- Highlights from the interim assessment
- Major categories of proposed solutions
- Next steps -- Implementation

Current Status of the Project

- 34 teams have submitted final reports
  - Assessment of Variation and Analysis of Solutions
  - Final Implementation Plan
- Summary and Analysis of those reports is underway
- Final Summary Reports are due to AHRQ and ONC May 15th
- Final Nationwide Summary due to AHRQ ad ONC June 30th

Sources of Variation

- Variation Related to Misinterpretation and Misapplication of Federal Laws and Regulations
  - HIPAA Privacy Rule
    - Minimum Necessary
  - HIPAA Security Rule
    - Decisions about appropriate security practices
    - Knowledge about what is available

Sources of Variation

- Variation Related to State Privacy Laws
  - Scattered throughout many chapters of law
  - When found, it is often conflicting
  - Antiquated-written for a paper-based system
- Trust in Security
  - Organizations
  - Consumers/Patients
- Cultural and Business Issues
  - Concern about liability for incidental or inappropriate disclosures
  - General resistance to change; importance of human judgment

4 Major Categories of Proposed Solutions

- Practice and Policy
  - organizational interoperability – e.g., Adopt a uniform consent policy
- Legal and Regulatory
  - modify state statutes to resolve differences regarding *when* and *how* patient consent is obtained and documented
- Technology and Data Standards
  - standard data format to document consent that recognizes the differing state-based consent policies, laws and regulations yet promotes normalization and interpretation
- Education and Outreach (organizations and consumers)
  - Practices, Policies, and Expectations

Frequency of Recommended Solutions

Interim Report Solutions Categories	N (%)
Develop mechanisms to engage and educate consumers on HIE, health IT, privacy and security of health information and their rights, roles and responsibilities	25 (74%)
Adopt standards for authentication, authorization, access controls, audits	24 (71%)
Develop standardized patient consent forms, policies and processes at the state level	20 (59%)
Adopt standardized patient identification methods (including a patient identifier, patient ID verification, a patient identification system)	18 (53%)

Frequency of Recommended Solutions

Interim Report Solutions Categories	N (%)
Establish governance/leadership groups to address privacy and security issues as well as state/regional HIE initiatives	16 (47%)
Modification of state laws/regulations (addressing patient consent, medical record statutes, HIE initiatives, sensitive health information, emergency situations)	15 (44%)
Pursue clarification/recommend changes to other federal regulations (CLIA, mental health, substance abuse, FERPA, etc)	14 (41%)
Address issues related to the disclosure of sensitive health information (eg the need to segregate sensitive data creates a challenge to role-based access)	12 (35%)

Frequency of Recommended Solutions

Interim Report Solutions Categories	N (%)
Address differences between HIPAA Privacy and State Law	12 (35%)
Adopt standards for secure transmission, digital/electronic signatures, data/document integrity, remote access	11 (32%)
Standardization of HIE-related Forms and Practices/Policies (BAA forms, HIE Participating Agreement Forms)	10 (29%)
Develop guidance and education for health care providers, other health care organizations	10 (29%)

Frequency of Recommended Solutions

Interim Report Solution Category	N (%)
Address government reporting and HIE participation (public health, medicaid)	9 (27%)
Address HIE issues between health care organizations and specialized units of government (law enforcement, correctional institutions)	7 (21%)
Establish interstate leadership group to address state-to-state HIE issues	4 (12%)

Sampling of Key Areas of Focus for Implementation

- 4 A's
  - Defining and adopting standard user and entity authentication and authorization protocols
  - Developing a standard minimum auditing policy that identifies security relevant events
  - Role-based Access
- Defining method of appropriately segregating data and working through the challenge for appropriate role-based access
- Identifying a standard, reliable method of accurately matching records to patients
- Defining a core minimum EHR data set

Example of One Approach to 4 A's

- **Authorizing** individuals to access patient data
- **Authenticating** individuals when accessing patient data
- Setting **Access controls** to appropriately limit authorized individuals' access to patient data
- Coordinating **Auditing** activities across organizations to assure patient data has not been inappropriately accessed

Work Group Charge

- Develop a conceptual solution that describes the characteristics or requirements for a solution for each of the 4As
- Identify specific policies, procedures, mechanisms or technologies that met the characteristics or requirements
- Develop action plans to implement the policies, procedures, mechanisms or technologies identified as solutions

Principle Development

- Develop a set of principles for authorizing and authenticating individuals, setting access controls, and auditing in a HIE, that are:
  - Agnostic with regard to specific technologies or HIE architectures
  - Time invariant to avoid obsolescence
  - Scaleable to accommodate small and large HIE models

Additional Work Group Considerations

- The results, work products, and standards from other state and national groups and projects
- The healthcare industry's on-going experiences with defining and implementing particular architectures and networks
- Technological changes that provide enhanced ability to implement technology solutions
- "Best practices" and "lessons learned" as health care organizations gain experience in implementing exchanges

4 High Priority Principles

1. P3.1 (Access Controls) - Health care providers should only access information for patients with whom they have a treatment relationship and then only the health information relevant to the treatment being provided.
2. P3.2 (Access Controls) - All organizations participating in a Health Information Exchange should develop and accept written policies and procedures for accessing and exchanging patients' health information through the HIE.

4 High Priority Principles

3. P1.4 (Authorization) - All organizations participating in a Health Information Exchange should develop and accept security credentialing guidelines for authorizing individuals to access patients' health information through a Health Information Exchange. The security credentialing guidelines and process should be as streamlined as possible and minimally include:
   - a) verifying the identity of individuals authorized to access/exchange health information
   - b) defining the appropriate role-based access for individuals authorized to access/exchange health information
   - c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.

4 High Priority Principles

4. P4.1 (Auditing) - All organizations participating in a Health Information Exchange should develop and accept minimum standards for routine auditing of individuals' access to patients' health information through the Health Information Exchange.

Moving Forward

- State Project Teams
  - State Task Forces and Central Coordinating Bodies
  - Introducing state legislation
  - Continuing to work collaboratively

Thank You

More Information:

http://Healthit.ahrq.gov/privacyandsecurity

www.rti.org/hispc

Report on the Approach to the 4 A's

www.health.state.mn.us/e-health/mpsp