

Privacy and Security Solutions For Interoperable Health Information Exchange

April 26, 2007

Presented by:
Linda Dimitropoulos,
John Loft,
Barbara Massoudi,
RTI International

Moderator:
Erin Grace, AHRQ



Privacy and Security Solutions For Interoperable Health Information Exchange

Project Overview
Methodology
Assessment of Variation and
Analysis of Solutions

Presented by:
Linda Dimitropoulos
John Loft
Barbara Massoudi



Overview of Today's Session

- Overview of the Project
- Methodology
- Interim Assessment of Variation and Analysis of Solutions



Background

- Variation in privacy and security business practices and policies creates a barrier to electronic clinical health information exchange
- The existing paradigm for privacy and security protections does not fully accommodate active consumer participation in health information exchange
- Consumers, organizations, and state and federal entities share concerns related to maintaining the privacy and security of health information



Assumptions

- Decisions about how to protect the privacy and security of health information should be made at the local community level
- Discussions need to take place to develop an understanding of the current landscape and the variation that exists between organizations within each state, and ultimately across nation
- Stakeholders at the state and community levels, including patients and consumers, must be involved in identifying the challenges and developing solutions to achieve broad-based acceptance



Health Information Security and Privacy Collaborative

- Health Information Security and Privacy Collaborative (HISPC) includes 33 States and 1 Territory, Puerto Rico
 - 1 subcontracted organization per state
 - Each subcontracted entity was designated by the governor
 - Each state identified a steering committee which is a private-public partnership composed of leaders from state government and stakeholder organizations
 - Work conducted through series of work groups with specific charges



Project Tasks

- Identify the variation in organization-level business practices, policies, and state laws that creates barriers to eHIE
 - Identify practices and policies that serve as “checkpoints”
 - Document the rationale or “driver” behind the practice or policy
- Develop solutions
 - Incorporate the “good” practices and policies into proposed solutions
 - Work with stakeholders toward consensus-based solutions to harmonize the variation and create appropriate protections
- Develop a plan to implement the solutions



Project Outcomes

- Preserve privacy and security protections in a manner consistent with interoperable electronic health information exchange
- Incorporate state and community interests, and promote stakeholder identification of practical solutions and implementation strategies through an open and transparent consensus-building process
- Leave behind in states and communities a knowledge base about privacy and security issues in electronic health information exchange that endures to inform future HIE activities



Project Reports and Products

- Interim Reports
 - Assessment of Variation
 - Analysis of Solutions
 - Implementation Plans



Product Reports and Products

(continued)

- Project Toolkit
- National Meeting Proceedings and Presentation Slides
- HealthIT.AHRQ.gov/privacyandsecurity
- www.rti.org/hispc



Project Reports and Products

(continued)

- Final Reports
 - Final Assessment of Variation and Analysis of Solutions Reports
 - Final Implementation Plans
 - Final Nationwide Summary



Methodology



Purposes of the Methodology

1. Assess variations in organization-level business practices, policies, and state laws that affect health information exchange
2. Identify and propose practical solutions, while preserving the privacy and security requirements in applicable federal and state laws
3. Develop detailed plans to implement solutions



Assumptions Underlying the Methodology

- Decisions about protecting the privacy and security of health information should be made at the local community level
- Discussions need to take place to develop an understanding of the current landscape and the variation that exists between organizations within each state, and ultimately across states
- Stakeholders at the state and community levels, including patients and consumers, must be involved in identifying the challenges and developing solutions to achieve broad-based acceptance



Overview of the Process

- Community-based research model where states “own” the issues and outcomes
- Engage broad range of stakeholders to identify challenges and develop solutions
- State project teams follow a “core” methodology that frames discussions in terms of purposes for the exchange of certain types of health information within 9 domains of privacy and security



Overview of the Process

- Each state assembled a steering committee, and work groups charged with
 - Assessing variations and identifying barriers to privacy and security (Variations Work Group)
 - Identifying legal/regulatory drivers (Legal Work Group)
 - Identifying solutions (Solutions Work Group)
 - Develop plans to implementation solutions (Implementation Planning Work Group)



Exchange Scenarios

- Relate to Purposes of Health Information Exchange (18 Scenarios)
 - Treatment
 - Payment
 - RHIO
 - Research
 - Law Enforcement
 - Prescription Drug Use/Benefit
 - Healthcare Operations/Marketing
 - Bioterrorism
 - Employee Health
 - Public Health
 - State Government Oversight



Nine Domains of Privacy and Security

- User and entity authentication
- Authorization and access controls
- Patient and provider identification
- Information transmission security and exchange protocols
- Protection against improper modification
- Information audits
- Administrative or physical security
- State law restrictions
- Information use and disclosure policies



Stakeholder Outreach

- Providers
- Payers
- Federal health facilities
- State government
- Hospitals
- Public health agencies
- Community clinics and health centers
- Laboratories
- Pharmacies
- Long term care facilities and nursing homes
- Homecare and hospice
- Correctional facilities
- Professional associations and societies
- Medical and public health schools that undertake research
- Quality improvement organizations
- Consumers or consumer organizations



Methodological Toolkit

- Scenarios describing situations calling for exchange of health information
- Template and data base for recording business practices consistently
- Operations manual including guides for conducting stakeholder meetings
- Appendices:
 - Reference Library
 - Legal Requirements for Health Data Exchange
 - IT Security Primer
 - Glossary of Terms



Variations Work Group and Stakeholder Groups

- Work group meetings discussed scenarios and generated a core set of business practices and policies for each scenario
- Reviewed core practices and policies by broader range of stakeholders to validate the business practices and fill gaps
- Coded practices as barriers to interoperable health information exchange (or not)



Legal Work Group

- Reviewed “barriers” to determine legal basis for the practice or policy
- The term “law” used here refers to relevant regulation, statute, or case that is the primary underlying driver behind a business practice



Solutions Work Group

- Identified Range of Feasible Solutions
 - Legal or Regulatory
 - Business Practice or Policy
 - Technology
 - Education or Guidance



Implementation Planning Work Groups

- Developed plans to implement solutions
- Next Steps
 - Leadership/Governance
 - Responsibilities
 - Resource requirements
 - Schedule
 - Outcomes



Regional Meetings

- 10 meetings held throughout the country in October and November of 2006
- Included HISPC states as well as other states — Representatives from 42 states and Puerto Rico
- Opportunity to collaborate
 - On common intra-state issues
 - On inter-state issues
- Format: Presentations with breakout sessions



Regional Meetings

- Both the Regional and National Meetings are integral components of the project methodology
- Opportunity to share results of the variations assessment and solutions development
- Opportunity to look across state borders to consider interstate health information exchange



Regional Meetings

- **Top Five Themes**
 - Variations in Patient Consent, Authorization (must all, opt-in, opt-out, no-opt)
 - Lack unique patient identification method/system across state/region/nation
 - Addressing the "4 A's" — Authentication (Identification), Authorization, Access Control, Audit across all means of infrastructure disclosure
 - Varying interpretations of HIPAA privacy and state laws and variations in the implementation of HIPAA security specifications (Administration, Physical, Technical, Human)
 - Interstate HIE issues: federal and state laws addressing (or not) interstate exchange of PHI



National Meeting

- Held in Bethesda, MD, March 5–6, 2007
- Opening remarks from Dr. Carolyn Clancy (AHRQ) and Dr. Robert Kolodner (ONC)
- Included HISPC states as well as other states
- Format included presentations and breakout sessions



National Meeting

- Breakout sessions encouraged collaboration on
 - Consent Issues
 - Data Security and Quality
 - Legal and Regulatory Issues
 - Interpreting and Applying HIPAA
 - Reducing Mistrust through Education and Outreach
 - Moving Forward from Different Points in the Process
 - Governance and Leadership for Privacy and Security Solution
 - State Legislation and Business



Interim Assessment of Variation Report

... the interim reports are but a "snapshot" of a point in time in an evolving process...



Sources of Variation

- Variation Related to Misunderstandings and Differing Applications of Federal Laws and Regulations
 - HIPAA Privacy Rule
 - Patient Authorization/Consent
 - Variation in Determining "Minimum Necessary"
 - HIPAA Security Rule
 - Confusion regarding the different types of security required
 - Misunderstandings regarding what was currently technically available and scalable
 - CFR 42 part 2
 - Variation in the treatment facilities', physicians', and integrated delivery systems' understanding of 42 CFR pt. 2, its relation to HIPAA, and the application of each regulation



Sources of Variation *(continued)*

- 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



Sources of Variation *(continued)*

- Variability in the use and implementation of patient consent or authorization across organizations
 - Lack of understanding about when federal and state laws require patient consent
 - Lack of a standardized requirement for when to use patient consent
 - Lack of a standard form to be used in connection with patient consent and authorization



Sources of Variation *(continued)*

- Variability in the interpretation and application of the “Minimum Necessary” standard
 - Widespread belief that it applies to disclosures to providers for treatment purposes
 - Lack of models and best practices for applying “Minimum Necessary” in all other non-treatment-related disclosures
 - Increases the time required for the exchange and affects the ability to receive comprehensive records



Sources of Variation *(continued)*

- Lack of a standard, reliable way of accurately matching records to patients
- Lack of standard authentication and authorization protocols
- Inability to appropriately segregate data poses a challenge to appropriate role-based access
- Current lack of auditing capability because of technical inadequacies and nonexistent or poor audit programs



Interim Solutions Report

... the interim reports are but a “snapshot” of a point in time in an evolving process...



Interim State-based Solutions

- Practice and Policy Solutions
 - Interpreting and applying HIPAA: “Minimum Necessary” Standard
 - Uniform consent
 - Policies to govern interstate exchange
- Legal and Regulatory Solutions
 - State laws: Finding and interpreting them
 - State laws governing secure exchange of health information
 - State laws and federal regulations regarding protected information



Interim State-based Solutions

(continued)

- Technology and Data Standards
 - Data security, quality, and transmission
 - Patient identity management systems
 - Segmenting data
 - Standards that affect technology
- Education and Outreach
 - Consumer education
 - Provider education



Interim State-based Solutions

(continued)

- Implementation and Governance
 - General implementation and governance issues
 - Governance and implementation of eHIEs
- Ancillary Issues and Solutions



National Level Recommendations

- National Standards
- Clarifications/Revisions to Federal Regulations
- Funding



Interim Implementation Report

... the interim reports are but a "snapshot" of a point in time in an evolving process...



Implementation Plans

- Governance and leadership
- Business practices and policies solutions
- Legal and regulatory solutions
- Technological and data standards solutions
- Education and outreach plans


