

MN Privacy & Security Project

Preliminary Findings and Next Steps

Billie Zippel – Chair, Variations WG

Laurie Beyer-Kropuenske – Chair, Legal WG

James Golden – Project Director, MPSP

September 8, 2006

Work Group Activities

- Variations WG
 - 6 Meetings – 15 hours of discussion
 - Reviewed 18 scenarios from RTI
 - Discussed and analyzed current and emerging models of health information exchange
 - Identified recurring privacy & security concerns

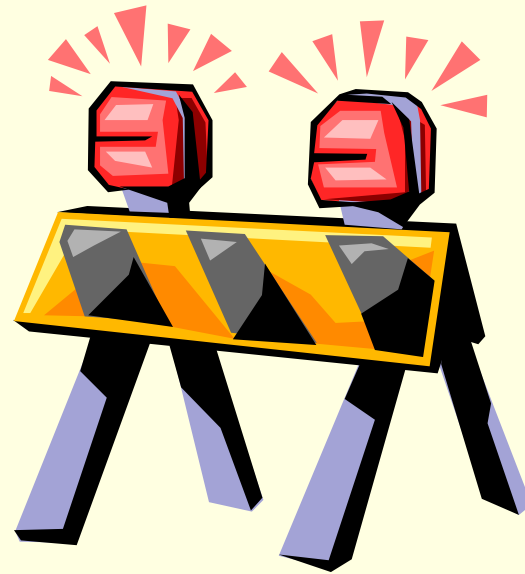
Work Group Activities

- Legal WG

- 5 Meetings – 12+ hours of discussion
- Focused on patient consent requirements in Minnesota law
- Discussed consent and liability issues within health information exchange
- Identified significant variations in current interpretation of Minnesota law

Key Privacy & Security Issues

- Implementation of Minnesota's requirements for patient consent to release health records
- Liability concerns with unauthorized or inappropriate disclosures of health information
- Operationalizing user authorization, information access controls, and auditing protocols



Barriers and Issues

Patient Consent Issues

- Patient consent provides individuals control over their health information
- Health information exchange requires general agreement on:
 - When patient consent is needed
 - How patient consent is obtained and documented
 - Mechanisms for exchanging or communicating the details of a patient's consent between organizations

Patient Consent Issues

- There are significant variations in:
 - The interpretation of current patient consent requirements in Minnesota law
 - Health care organizations' implementation of patient consent requirements – for paper or electronic exchange of health information
 - Organizations' belief about when and how patient consent must be implemented into health information exchange

Example of Variations

Patient Consent

- What is “Current Treatment” in M.S. § 144.335?
- 2+ very different interpretations of “Current Treatment” (see handout)
- These differing interpretations have significant implications for:
 - How patient consent is incorporated into HIE
 - Privacy protections provided through individuals’ control of their health information

Other Issues

Patient Consent

- “Health Record” not defined
- “Emergency” not defined
- Disclosing entity needs patient consent to disclose, but:
 - Patient is at the requesting entity’s location
 - Organizations do not have the ability to electronically exchange consent
 - Disclosing entities want to manually review patient consent prior to providing information

Liability Concerns

- Disclosing entities bear all responsibility for the appropriateness of health information disclosures
- Liability concerns make organizations conservative in how and when they disclose health information
- When in doubt about the appropriateness of a disclosure – organizations request consent

Liability Concerns

- Disclosing entities cannot rely on requesting provider's representation of having appropriate patient consent
- Addressing liability through contracts only minimally reduces liability concerns:
 - Contracts cannot fix damage to reputations
 - Differences in appropriate sanctions across organizations

Authorization, Access Controls & Auditing

- These issues are often architecture and model specific, but general concerns remain the same
- Paper controls do not translate well to electronic controls
- Most current controls are behavioral controls in policy rather than system controls

Authorization Issues

- Current HIE is often between two organizations and as more of the arrangements are developed:
 - User IDs, Passwords & Security fobs proliferate
 - Organizations need mechanisms to manage who is authorized to access information and what information can be accessed
 - As the number of entities involved in HIE increases so does complexity of user authorization without a central coordination

Information Access Control Issues

- Strong information access controls require a lot of knowledge of who will need access to what information:
 - However, information about providers' treatment relationships to patient may not be known in advance
 - It requires significant work and effort to maintain appropriate controls
 - Strong access controls can enhance privacy, but interfere with normal workflows

Information Access Control Issues

- Reliance on role-based access and policies to control access to information requires
 - Mechanisms for effective auditing of information access
 - Appropriate sanctions for inappropriate access
 - Clear policies and good user training and education

Auditing Issues

- Auditing identifies problems after the fact and does not limit inappropriate access
- Current auditing tools are blunt instruments because:
 - Auditing generates tremendous volumes of data
 - Effective auditing requires knowing who should be accessing what information
 - Most auditing today is complaint-based auditing
- We need more effective, intelligent auditing tools that can automate the process and take the place of humans



Documenting Findings

Privacy and Security Barriers Report Description

- The Privacy and Security Barriers Report is a descriptive report that:
 - Identifies the most significant privacy/security barriers
 - Clarifies the reasons and causes for the privacy/security barriers
 - Explains the implications of privacy/security barriers on HIE
- The report serves as a starting point for the Solutions and Implementation Plans WG

Privacy and Security Barriers Report Outline

- Executive Summary
- Background & Purpose
- Methodology
- Privacy and Security Barriers to HIE
 - Implementation of Patient Consent Requirements
 - Concerns of Liability for Inappropriate disclosures
 - Ability to Implement Appropriate User Authorization, Access Controls, and Auditing Protocols
- Conclusions
- Appendices



Next Steps

Solutions and Implementation Plans WG

- The Work Group will be asked to:
 - Eliminate or reduce the identified privacy/security barriers
 - Provide health care organizations flexibility in implementing electronic exchange of health information
 - Maintain and provide appropriate privacy and security protections for individuals' health information.

Solutions and Implementation Plans WG

- The Work Group will have ~ 40 individuals in two subgroups:
 - Patient Consent Subgroup
 - Authentication and Access Controls Subgroup
- Time Commitment
 - October – December: Bi-Weekly Work Group Meetings
 - January – February: Ad-Hoc Work Group Meetings (as needed)
 - Meetings will be 2 hours

Solutions and Implementation Plans WG

- Members of the Work Group should provide expertise in:
 - The development and implementation of privacy policies and procedures
 - Information system development and the implementation of security policies and procedures
 - Consumer and patient advocacy

Solutions and Implementation Plans WG

- Members for the Work Group invited from:
 - MN e-Health Advisory Committee Recommendations
 - Variations and Legal Work Group
 - Health Care Associations
 - Consumer and Privacy Advocates
 - Other stakeholders not currently participating
- Recommendation – Vendors may participate, but not as Work Group members

Thank You! - Questions

Key Contacts for More Information:

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

Minnesota Department of Health

Jim Golden, PhD – MPSP, Project Director

651.201.4819

james.golden@health.state.mn.us