Minnesota’s e-Health Initiative: Privacy and Security and modifications to the Minnesota Health Records Act

2008 State Alliance for e-Health meeting
Washington DC.
September 26th, 2008

Scott Leitz
Assistant Commissioner
Minnesota Department of Health
Topics for Discussion

- Minnesota e-Health Initiative
- Minnesota Privacy and Security Project
- Changes to Minnesota Law resulting from Project
- Next Steps
The Minnesota e-Health Initiative

A public-private collaboration established in 2004

- Legislatively chartered
- Coordinates statewide EHR/Health Information Technology-related policy
- Develops and acts on statewide e-health priorities
- Reflects the health community’s strong commitment to act in a coordinated, systematic and focused way
Minnesota e-Health Initiative Vision

“… accelerate the adoption and effective use of Health Information Technology to improve healthcare quality, increase patient safety, reduce healthcare costs, and enable individuals and communities to make the best possible health decisions.”

Source: e-Health Initiative Report to the MN Legislature, January 2004
A Summary of Key Executive and Legislative Milestones for Minnesota e-health

2004: Minnesota e-health initiative established
E-Health Steering Committee formed, outlines vision and roadmap for strategic action

2005: MN e-Health Advisory Committee created: 4 year commitment of statewide leadership

2006: Governor Proposed $12 Million in matching grants. Legislature Funds $1.5 Million for 2006.

2007: Governor Proposes $29.5 Million in matching grants; Legislature Funds $14.5 Million Grants & Loans for 2007/08
A 2015 Mandate for Interoperable EHR’s established
Law to create a statewide Implementation Plan (out June 26/08)
Law to establish uniform standards by 2009
Revised and recodified the Minnesota Health Records Act to update consent requirements for an electronic age.

2008: All EHR’s acquired must be certified
All providers must establish and use e-prescribing by 2011
Governor announces plan for PHRs for all state employees by 2009
Minnesota Privacy and Security Project (MPSP)

A systematic and comprehensive review of current laws and practices that impede the efficient, electronic exchange of health data that analyzed privacy and security issues to:

- Identify the most significant barriers impeding the electronic exchange of health information
- Document how concerns impede the exchange of health information
- Describe the causes and rationale for the barriers
- Develop solutions and implementation plans to eliminate or reduce the barriers, while maintaining or strengthening patient privacy protections
MPSP Findings

🎯 Overarching privacy and security issues:
- The implementation of Minnesota’s patient consent requirements within a health information exchange
- Operational difficulties in first providing, and then limiting and monitoring external organizations’ electronic access to patient data
- Liability concerns with the inappropriate disclosure of patients’ health information
Patient Consent Barriers

- Minnesota’s patient consent requirements were identified as a major privacy and security impediment to the electronic exchange of health information, because:
  - Health care providers cannot agree on “when” and “how” patient consent is required to exchange patients’ health information.
  - Minnesota’s patient consent requirements were designed for paper-based exchanges of information and are not conducive to a real-time, automated electronic exchange of information.
Patient Consent Requirements

- HIPAA allows the disclosure of patient information for treatment, payment, and operations without consent.

- Minnesota law requires patient consent for the disclosure of patient information.
Minnesota’s Patient Consent Requirements

- Patient consent required for nearly all disclosures of health records – **including treatment**
  - Patients need to give written consent
  - Consent generally expires within one year
  - Limited exceptions to consent
    - Medical emergency
    - Within “related health care entities”
  - Consents that do not expire
    - Disclosures to providers being consulted
    - Disclosures to payers for payment
Minnesota Patient Consent Liability

- Minnesota law places all liability for inappropriate disclosures on the disclosing providers:
  - A violation of patient consent requirements may be grounds for disciplinary action against a provider by the appropriate licensing board or agency
  - A person who negligently or intentionally releases a health record … is liable to the patient for compensatory damages caused by an unauthorized release, plus costs and reasonable attorney's fees
Minnesota Patient Consent Barriers

- **Undefined terms and ambiguous concepts** in Minnesota Statutes, § 144.335.
- Difficulties in determining the appropriate application of Minnesota’s patient consent requirements to new concepts in the electronic exchange of health information that do not have an analogous concept in a paper-based exchange.
- The need to update Minnesota’s patient consent requirements to allow mechanisms that facilitate the electronic exchange of patients’ information while respecting the patients’ ability and wishes for controlling their information.
Addressing Patient Consent Barriers

A workgroup of industry representatives and privacy advocates did not reach consensus on a set of best solutions, but:

- Identified options
- Documented advantages and disadvantages for each option
- Connected related options

MDH developed criteria for evaluating options:

- maintain or strengthen patients’ privacy or control over their health records
- improve patient care
- facilitate electronic, real time, automated exchange
- not place an undue administrative burden on the health care industry
- increase the clarity and uniform understanding of the statutory language and consent requirements
2007 Revisions to MN Health Records Act

★ Major Revisions:
– Improve readability through recodification
– Definitions for new and existing terms:
  • Health record
  • Medical emergency
  • Related health care entity
  • Health information exchange
  • Record locator service
  • Identifying data
Record Locator Service (RLS)

- An electronic index of patient identifying information that directs providers in a health information exchange to the location of patient health records held by providers and group purchasers.
  - Providers **may construct** a record locator service **without** patient consent
  - Providers **must obtain patient consent to access** patients’ information in a record locator service.
Record Locator Service Protections

- Not a government database
- Allows multiple groups of providers to create a RLS
- Only providers may access information in a RLS
- Providers must provide patients the ability to completely opt-out of the RLS in the consent process
- An RLS must maintain an audit log of who accessed information
- A RLS is liable for inappropriate disclosures of information
- MDH cannot access/receive information from a RLS
Representation of Consent

A provider, or a person who receives health records from a provider, may not release a patient's health records to a person without:

(1) a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release;

(2) specific authorization in law; or

(3) a representation from a provider that holds a signed and dated consent from the patient authorizing the release.
Representation of Consent Protections

- **Only a health care provider** may request a patient’s health record using a representation of having obtained patient consent.

- **Requesting provider must obtain** a signed and dated consent from the patient.

- The provider releasing health records to another provider using a representation of having obtained patient consent **must document:**
  - identity of the requesting provider
  - identity of the patient
  - records requested
  - date of the request
Thank You! - Questions

Minnesota Department of Health
Scott Leitz
651.201.3565
Scott.leitz@state.mn.us