

Applying the 4A Principles: Exchanging a Clinical Abstract

Dan Routhe
AHRQ Project Coordinator

June 28, 2007

Project Background

- Three-year project
- Four Partners – Allina, Fairview, HealthPartners, and the University of Minnesota
- Three forms of exchange
 - Level 1 – patient controlled (opt in) sharing of an abstract. Uses Epic's MyChart
 - Level 2 – Epic, acting as a RLS, determines if the patient has clinical information within the partnership (opt out)
 - Level 3 – exchange clinical information with a non-Epic EHR

Rationale for the abstract

- Contents are bounded & defined
 - A better first step for a public wary of confidentiality breaches
 - Patients “get it.” They immediately understood the value of “My Emergency Data” for themselves and their providers
 - Greater patient acceptance
 - Its succinctness is preferred by emergency room physicians
 - Interoperability across vendor platforms
- Can be viewed as a document from its health system source
- Our abstract
 - Level 1 (Epic’s MyChart) “My Emergency Data”
 - Level 2 (HL7’s CCD) “My Clinical Summary”

The Level 1 Abstract: My Emergency Data

- Patient Information
- Contact Information
- Primary Care Physician & Center
- Advanced Directives
- Current Problem List
- Current Medications
- Allergies
- Immunizations
- Surgical History
- Family Medical History
- Alcohol and Tobacco use

Exchanging abstracts: key issues

- Gaining the patient's consent for disclosure
- Breaking the glass
- Matching patients across health systems
- Authenticating the requestor
- Access control for requesting abstracts
- Audit trails
- Technical communication, messaging, transfer and error handling

First steps to applying the principles

- Discuss the principles with the partners
- Categorize the principles
 - Technology based
 - Covered by Minnesota laws
 - Covered by existing policies
 - Similarities
 - Differences
 - Develop new policies
- Apply the principles to current business practices of sharing patient data
 - Start with the five most important, as determined by the 4A work group

Discuss the principles with the partners

- First with members of the Executive Board
 - Upper level management
- Next with the Project Implementation Committee
 - Make up: doctors, nurses, IT personnel and other specialists
 - Determined to form a special committee made up of:
 - project coordinator
 - three local project coordinators
 - representatives of the medical records personnel from each of the partners
 - Concentrate on the five most important principles as determined by the 4A work group
 - P1.4, P3.1, P3.2, P4.1 and P4.2

Categorize the principles

- Technology based
- Covered by Minnesota law
 - Current
 - Proposed under new legislation
- Covered by existing policies
 - Map similarities and differences between the partners
- Need to develop new policies

Technology based

P4.2 - All organizations participating in a Health Information Exchange should maintain audit logs that document individuals accessing patients' health information. The audit logs should minimally identify: a) the individual accessing the health information; b) the health information being accessed; c) the date and time of the access; and d) all failed log-ins.

- Data to be captured:
 - Data to be included on the request should include, Requestors unique user-id, first and last name of the requestor, the institution represented by the requestor, time/date of the request and verification that the requestor has the patients consent.
 - Data returned to the requestor should include, time/date stamp, name of the sending institution, user-id of the requestor.

Covered by Minnesota laws

P3.2 - 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 Health Information Exchange.

- Access to a patient's health information is acceptable under the following conditions (this is taken from proposed Minnesota statute 144.293 subdivision 3 and current Minnesota Statute 144.335 subdivision 3):
 - A patient's health record, including, but not limited to, laboratory reports, x-rays, prescriptions, and other technical information used in assessing the patient's condition, or the pertinent portion of the record relating to a specific condition, or a summary of the record, shall promptly be furnished to another provider upon the written request of the patient. The written request shall specify the name of the provider to whom the health record is to be furnished. The provider who furnishes the health record or summary may retain a copy of the materials furnished. The patient shall be responsible for the reasonable costs of furnishing the information

Covered by existing policies

— Similarities —

P3.1 - 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.

- The health care provider (requestor) shall maintain records that show the patient was under their care at the time of request, the treatment or service that was being provided, and if needed, a copy of the patient's consent form with a valid signature of the patient. These documents should be dated no later than the date of the request for information.

Covered by existing policies

— Differences —

- P1.4** - 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; and c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.
- This needs to be looked at from each participant's organization. The written rules by each should stay in effect when it comes to assigning levels of security within the parent organization. There needs to be a 'level' of security that will allow access to patient records outside of the parent organization, much the same as the 'level' that allows access inside the organization.

Need to develop new policies

P4.1 - 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.

- Patient's records should be audited on a periodic schedule looking for an unusual number of requests:
 - for a specific patient's data
 - by a specific user-id
 - by an institution
 - over a short time frame

Next steps

- Continue the process with the remaining 14 principles.
- Develop a comprehensive document that all partners agree with.
- Submit the document for legal review within the partners.
- Determine the changes that need to be implemented in each partners policies and work flows.
 - Remember that the existing paper based system will remain in place for the foreseeable future.
 - Determine how to apply the agreement to the existing system.
- Bring the document to a prospective Level 3 partner.
- Continue to meet as a group.

Conclusion

- The principles work well as a roadmap
- There has to be buy-in from upper management
- Choose the work group members wisely
- One person should coordinate the efforts
- Look at current policies first
- An abstract eased the application of the principles

Thank you

Contact Information

Dan Routhe

Routh007@umn.edu

612-625-3512