Technology Aspects of Health Information Exchange

Steven E. Labkoff, MD, FACP
Director, Pfizer Healthcare Informatics
Pfizer’s Fair Health IT Principles

- **Patient First:** Patients’ rights and needs must drive the evolution of HII. Essential patient interests include safety, quality, individualized care, privacy, public health, and access to care.

- **Clinical Judgment:** HII should provide greater access to data and support to enable the provider to make better healthcare decisions in collaboration with the patient.

- **Healthcare Cost Awareness:** New technologies should be used to reduce total costs in healthcare, by improving understanding of long-term costs and outcomes, reducing errors and redundancies, and increasing efficiency.

- **Rigorous Standards for Healthcare Information:** All parties disseminating information that influences patient outcomes should be subject to equivalent rigorous standards of research, presentation and communication.

- **Shared Responsibility:**
  - **Shared Governance:** All healthcare stakeholders must share the burden of creating and enforcing efficient processes and robust safeguards within HII to assure the adoption of systems aligned with the provision of quality care.
  - **System Affordability:** HII must advance in such a way that no stakeholder is unduly burdened by the costs of purchasing technology and constructing infrastructures.

- **Integrity in Technology:**
  - **Neutral Platform:** HII should be provided through neutral platforms that support honest brokers. It should not advance the commercial interests of any party to the potential detriment of patients.
  - **Interoperability:** HII must conform to prevailing quality and technical standards to facilitate adoption and control costs, but also be flexible to support innovation and improvements.
Agenda

- The Need for Technical Architectural Standards
- Technical Issues of HIE
- The Patient/MD Connection
- The RHIO-to-RHIO/NHIN connection
- Existing Authentication Models
- Q&A
Make it “Thin”

Avoid “Rip and Replace”

Separate Applications from the Network

Decentralization

Federation

Flexibility

Privacy and Security

Accuracy
Support clinicians and patients with interoperable electronic health record (EHR) systems,

Computerized provider order entry (CPOE),

Clinical decision support systems (CDSS) for the purpose of improving the quality, safety, and efficiency of healthcare for patients and providers.
eHI’s Vision of HIE

A network through which all authenticated participants may securely exchange information without loss of meaning:

- All message senders and receivers are authorized and authenticated.
- All messages are signed and encrypted.
- All messages are actively acknowledged or rejected by the receiver in real time.
- All messages meet conformance tests for use case specific standards that can support the exchange of clinical information between disparate information systems capable of different levels of interoperability.
- All information is exchanged in accordance with a set of principles, policies, and procedures to which each participant has agreed in a binding contract.

http://toolkit.ehealthinitiative.org/technology/common_principles.mspx
Standards

Legacy Systems

Variations on implementations (ie: HL7 variations) of data messaging

Lack of agreements between partnering organizations

Funding models to support overall infrastructure
**Technical Aspects of RHIOs**

- **Several Emerging Venues**
  - State-wide
  - City-wide
  - Community-wide

- **Multiple Architectures Developing**
  - NHIN Contracts: CSC, Acenture, IBM, Norfolk Grumman

- **Major issues**
  - Authentication: People, applications, processes
  - Privacy
  - Speed
  - Identification
  - Buy in

---

**Technology is SELDOM the rate limiting step**
Federated (Centralized) Model: Schematic of (Indianapolis)
Federated (Distributed) Model: Patient Safety Institute
Despite central DB, individual hospitals can shield contracting & financial data.
Dark fibers connect core constituents; community has net access.
Peer-to-Peer, Indexed Model

Schematic of SBCCDE

- Ambulatory Care EMR
- Regional Hospital HIS System
- Laboratory System
- Public Health System

- query path
- data connection utilizing resulting pointers to systems

MPI
Definition:

Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. “www.pki.vt.edu/help/glossary.html”
Policy & Identity Approach

Policies, Procedures, Standards & Guidelines (PPS&G)

PPS & G

Core Security Policies
A select number of controls (usually ISO 17799) are identified to be relevant for the project. A core set of policy, procedural, standards and guideline documents to support those controls will be developed.

Identity Management
For many health care settings, there are two distinct identity types in the project: identities as subjects (patients) and identities as users (system end-users). Managing these identities to ensure accuracy of patient data linkage, legitimate access control to data for users and administration across these identity types underpin this implementation and will be performed. Other types of identities and relationships may also need to be managed.
Access Control Approach

Authenticated User seeks to access Patient Data

Role Based Access Control
What Data Types or System Functions can be used by The User?

Patient Consent
Has the Patient consented To information being shared Outside of authoring Organization (if applicable)?

Patient Provider Relationships
Does a relationship exist Between the Patient and The User?

Access Control Framework

Registration
Authentication
Authorization

Role Based Access Control
Consent
Patient Provider Relationships

Pseudonymisation and Anonymisation
To enable use of data for secondary purposes
A user claims an identity and presents evidence to back up the claim. The evidence can be something the user knows has or does and the system evaluates the evidence using stored authentication information. If he present something he knows and something he has, that is termed “two factor” authentication. Authentication in networks must solve a broader problem.
Factors in Authentications

Something you know: Password
Something you are: Biometrics
Something you have: Token
Factors in Authentication

- **1 Factor: you know your username & password (these are 1 factor)**
  - Better than nothing but weak – can be copied easily

- **2 Factor: RSA Token + Password**
  - Much more secure and people feel good about it

- **3 Factor: Biometrics + Password + Token = 3 factors**
  - Ultra secure – not generally used (not all 3 together)
NIST Level 1: Public site, no authentication

NIST Level 2: A password known only to the user

NIST Level 2 or 3: A digital certificate; a secret key contained in a normal file

NIST Level 3: A physical Smart-Card or physical token

NIST Level 4: A biometric measurement such as a fingerprint
Authentication in a Single RHIO
Authentication in a Single RHIO
What happens when two RHIOs don’t use the same authentication process?
SAFE BioPharma Association

- Non-profit coalition sponsored by the Bio-Pharmaceutical industry
- Unique electronic identity credentials for legally enforceable & regulatory compliant digital signatures

SAFE

- Satisfies NIST Level 3
- 2 factor authentication; something you know & have (hardware cryptography)
- Provides credentialing and nonrepudiable digital signatures
- Closed user community, based on mutually agreed legal rules, to ensure global enforceability among participating entities
Anakam LLC

- For-profit, privately-owned security software firm
- Provides innovative solutions for identity management & authentication; particularly for online banking and ecommerce.

GoVirt Multifunction Authentication

- Satisfies NIST Level 3
- 2 factor authentication; something you know & have
- Completely software based; no additional hardware necessary
- 2nd factor authentication can be provided on multiple platforms; ie. mobile phone, voice technology, encrypted PC, etc.
PGP, Inc.

- For-profit, private coalition sponsored by the Bio-Pharmaceutical industry
- Global customer standard for encryption and digital-signature solutions

PGP Encryption Platform

- Satisfies NIST encryption standards
- Authentication via PKI & symmetric key (cryptographic signature)
- Suite of tools that can encrypt data, data storage, and mobile devices
- 2 Factor Authentication, but supports 1 or 2 factors – policy issue for organizations using this solution
General Services Administration (GSA)

- Government agency to help federal agencies serve the public by offering superior workplaces, expert solutions, acquisition services and management policies.
- Consists of the Federal Technology Service (FTS), the Federal Supply Service (FSS), and other offices…

E-Authentication

- Based on Security Access Markup Language (SAML)
- 2 Factor Authentication
- Can satisfy NIST levels 1-4
- Browser based protocol security
- Provides single sign on in a federated environment for application logon
eHI’s Technical Working Group

- Looking for volunteers to assist in vetting out some of the questions around technical issues concerning RHIOs
- Looking at technology proper and policy
- Goal is to add info to the eHI took kit
- Current leaders – Hugh Zettel, GE, Bob Steffel, Health Bridge

Contact Info
- Labkoff@pfizer.com
- 212-733-4766

Special Thanks to
Daijin Kim, Healthcare Informatics
Brian Kelly, Accenture
Ash Evans, SAFE Biopharma
Key Clients/ Partners:

- Bio-Pharma; AstraZeneca, BMS, GSK, J&J, Merck, Pfizer, etc.
- Governments; NCI, FDA, EU Medicines Evaluation Agency, etc.
- Research Site & IRBs; Mayo Clinic, Moffitt Cancer Center, etc.
- Vendors; Adobe, Bearing Point, IBM, etc.

Benefits:

- Real-time identity assurance
- Standards mandate identity proofing and registration in person
- Globally enforceable digital signature with authentication

Concerns:

- Limited adoption outside of Bio-Pharma
Key Clients:

- Not publicly available

Benefits:

- No additional hardware required; no additional costs for 2nd level
- 2nd level authentication can reside on various platforms; mobile phone, voice technologies, encrypted PC, wallet card
- Administration of authorization to determine security level
- Low cost implementation for large populations; ie. online banking

Concerns:

- Proprietary technology
Key Clients:

- 84% of Fortune 100
- Pharmaceutical, Manage Care Organizations, Medical Facilities
- Aerospace & Defense Companies
- Petroleum refining companies

Benefits:

- Published product source code for peer review
- No requirement for complex passwords
- PGP can also encrypt data and data storage devices

Concerns:

- Complexities of implementing PKI infrastructure
GSA E-Authentication

Key Clients/ Partners:

- Government portal applications

Benefits:

- Open standards and industry accepted protocols
- Ease of administration due to federated environment and single sign on
- Platform neutral

Concerns:

- Browser based security is susceptible to various types of attacks