Interoperability and Scalability: Security, Identity Management and Trust in Health Information Exchange

Pete Palmer, Security/PKI Architect, Wells Fargo
HIMSS RHIO Federation Work Group Lead

April 26th, 2006 – Liberty Alliance Workshop

• Goal 1: Inform Clinical Practice

• **Goal 2: Interconnect Clinicians:** Identify interoperability as a major milestone for achieving improved healthcare delivery; encourage regional healthcare information organizations (RHIOs) and a national health information network.

• Goal 3: Personalize Care

• Goal 4: Improve Population Health

Source - HHS Health IT Strategic Framework, July 21st, 2004
http://www.hhs.gov/onchit/framework/hitframework/framework.html
Regional Health Information Organizations (RHIOs)
What is a RHIO?

A Regional Health Information Organization (RHIO) is a nongovernmental, multi-stakeholder organization that enables the exchange and use of health information, in a secure manner, for the purpose of promoting the improvement of health quality, safety and efficiency.
RHIOs Must Be Trusted

The usual first question asked about a RHIO is, “Can I trust that my personal health information remains private and only used when needed by an authorized professional?”

If the answer is ‘No’, the RHIO is doomed to fail.
RHIO Trust Challenges

To ensure interoperability and trust, RHIOs need standards for

- Authentication
- Authorization
- Credentials
- Risk Assessment Criteria
- Assurance Levels
Electronic Authentication Basics

• Authentication is *not* Authorization
• Identity Proofing (Vetting) Procedures
• Credentials
• Identity Assertion
• Assertion Validation
Determining Authentication Requirements

- Perform Risk Assessments
- Identify Assurance Levels (Sensitivity)
- Apply Credential Standards
Federated Identities

- Identity Independent of Applications
- Identity Recognized by Multiple Organizations
- Enables Single Sign-on
- Enables Electronic Federations
Federated Identity Management

- Communities of Trust
- Standardized Credential Types
- Standardized Policies and Procedures for Issuing Credentials
- Common Credential Validation System
Components of Federated Identities

- Identity Credential or Token (Authentication)
  - Username/Password
  - Digital Certificate/Signed Data
  - Biometric

- Identity Attributes (Authorization)
  - Organization
  - Roles
  - Custom Information

- Federated Identity Management Standards
  - Liberty Alliance, SAML
  - Electronic Authentication Partnership (EAP)
  - PKI w/Bridge Trust Model
Internet2’s Shibboleth SAML Flow Architecture (Slide c/o Scott Cantor, The Ohio State University)

Knock, Knock

Who’s There?

Mary

v6597w54wd7 who?

v6597w54wd7 who?

Mary, faculty, contract:001

Let me in!
HIMSS = Information Management

HIMSS Unified Membership:
National Vision, Local Focus

The Right Organization for Deploying the Regional Health Information Organization (RHIO) Federation
The HIMSS RHIO Federation
The HIMSS RHIO Federation
Identity Credential Standards
The HIMSS RHIO Federation
Security and Trust Architecture

Approved Trust Service Providers

HIMSS RHIO Federation

RHIO 1

RHIO 2

RHIO 3

Internet

The Source for Healthcare Information
Example RHIO Application: ePrescribing

Insurance Info, Medication History - RxHub
Approved Trust Service Providers
Pharmacy Routing – SureScripts

HIMSS RHIO Federation

RHIO 1
Pharmacy Pick-up

RHIO 2
Home Delivery
Thank You.

Contact information:
Pete Palmer
pete.palmer@wellsfargo.com