Lessons Learned
Privacy and Security
Interoperability Enablers

12th International HL7
Interoperability Conference
May 14, 2011
Orlando, Florida

Stan Ratajczak
Group Director, Implementation Support Group
Canada Health Infoway
Security Features
Security Flaws
Overview of today’s session

• The Canadian context

• Privacy and security interoperability enablers
  – e-Prescribing

• Lessons Learned - Conclusions
The Canadian Context

Pan-Canadian EHR Infostructures as Peers
Distributed, Federated, Message Based
* Quebec’s health services laws include provisions that address privacy.

** Yukon’s ATIPP law extends to cover hospital and personal health information.
Privacy legislative landscape

• Overview of jurisdictional legislative frameworks
  – Provisions for information sharing for care and treatment purposes.
  – Obligations for;
    • Health Information custodians
    • Health Information networks etc.
  – Provisions for secondary use
  – Consent for collection NOT required
  – Patient Consent directives for use and disclosure
  – Public health disclosures
  – Several provisions for privacy breach notifications
Key Messages

• Privacy Legislative harmonization attempts
  – Pan Canadian Confidentiality Framework
  – Common understandings of the Pan-Canadian Health Information Privacy Group
  – What are the business drivers for harmonization attempts?

• Privacy legislation/regulatory/policy frameworks “will” evolve over time
  – Design for configurability – do not hard code policy
    • Consent models
    • Levels of granularity of a patients' consent directives
    • Configurable rules engines
    • Evolving requirements based on;
      – operational experience
      – Public and clinician opinion

• Challenges
  – Which legislation applies in context inter jurisdictional sharing
  – Similar versus equivalent data safeguard provisions
  – Multiplicity Information sharing agreements
  – Concerns re: repurposing of information, other jurisdictional practices
    • Health system and outcomes monitoring
  – Secondary use of Personal Health Information
Privacy and Security Technology enablers
E-prescribing case study
Aspects of Trust Models

What does trust entail?

Sample trust components

Technical

Governance & Policy
A prescriber can only be linked to a prescription if their credentials are issued & validated by either the SHIN or the DIS.

An inferred Trust model.
Relying party must implicitly trust the overall system.
They cannot directly validate the authenticity of the prescription or other parties.
Authentication of user needs to be linked to an e-prescription.
E-Prescribing interoperability challenges

**JURISDICTIONAL INFOSTRUCTURE**

**Point of Service Integration**
- Integration drives requirement for interoperability

**Non interoperable;**
- User credentials
- Authentication
- Authorisation

**End user adoption**
- Multiple sign-ins

**Sustainable operational costs**

**Varying assurance levels of authentication**

**No clear integration between Access Control and Audit and Logging**

**Using interoperability enablers to build trust and meet business requirements**

**Lack of harmonized ITSEC, IT and privacy Governance models, with external business partners**

**Building consensus on common specifications for interoperability**

**Migration planning for multiple point of service settings;**
- Physician desktops
- Acute care facilities
- Retail Pharmacies
Overview of e-Prescribing Privacy and Security Requirements

- Authenticity prescribers, prescriptions and dispensers across the EHR ecosystem
  - Interoperability of security mechanisms across multiple point of service settings is key
  - Common definition of trust model components, requirements and specifications where possible.
  - Multiple Trust Models = Multiple sets of security interoperability requirements
Interoperability Enablers – Federated Identity Management

JURISDICTIONAL INFOSTRUCTURE

- Registries Data & Services
  - Client Registry
  - Provider Registry
  - Location Registry

- EHR Data & Services

- Drug Information

- Physician Office EMR

- Physician/Provider

- Pharmacist

- Secure Health Information Network (SHIN)

- Assertion Token A
- Assertion Token B
- Assertion Token C

- Identity Service Provider

POINT OF SERVICE
Interoperability Enablers – Federated Identity Management

JURISDICTIONAL INFOSTRUCTURE

- Registries Data & Services:
  - Client Registry
  - Provider Registry
  - Location Registry

- EHR Data & Services

- Drug Information

- Secure Health Information Network (SHIN)

- Identity Service Provider

- Assertion Token A

- Pharmaceutical System

- Physician Office EMR

- Physician/Provider

- Pharmacist
Federated Identity Management allows:

- for the acceptance of a variety of credentials
- for use of identity media of choice (multiple assurance levels)
- identity portability
- reduction issuance and management of credentials (EMR-HIS)
Interoperability Enablers – Federated Identity Management

Federated Identity Management requires 2 types of interoperability

Technical
Requires semantic interoperability
Multiple technologies exchanging data based on well defined and stable interface standards

Policy Level
Ability of organizations to adopt common business processes and Policies.
i.e. Liability, identity proofing, vetting, accreditation, Transparency, compliance and Risk Management Frameworks
Interoperability enablers

• Federated Identity Management
  – Definition:
    • A shared platform and consistent processes for managing information about users: who they are, how they are authenticated and what they can access
    • Claims-based identity = a common way for applications to acquire the identity information they need from users inside their organization, in other organizations, and on the Internet
  – SAML V2 /Liberty Phase 1-2-3
  – WS-Security, Policy, Trust, Secure Conversation and WS-Federation
    • Specification defines mechanisms for providing security-token-based integrity and confidentiality on Web Service -- or SOAP -- messages.
    • Several security tokens are defined, as well as a mechanism for associating them with messages.
    • WS-Federation defines a framework for federation. Profiles will be developed subsequently to specify the details for implementation.
  – ACTIVE DIRECTORY FEDERATION SERVICES 2.0
  – WINDOWS CARDSPACE 2.0, & WINDOWS IDENTITY FOUNDATION
  – HL7 PASS – Access control Service & Audit logging
Interoperability enablers
Lessons Learned

• Lack of security & trust model interoperability affects deployment options and potentially adoption of new functionalities.

• Privacy and security solutions vary widely across the Healthcare Ecosystem.
  – Interoperability MUST be defined as a key requirement
  – Build consensus on a common baseline set of requirements
  – Outcomes of your current state assessment

• Development of harmonized e-prescribing specifications
  – Drug Information Systems
  – Physician EMRs
  – Retail Pharmacy Applications
  – 2 Security Models to be defined at the requirements level
Interoperability enablers
Lessons Learned

• Constantly evolving business, technological interoperability requirements
  – Anticipate and design for change - configurability (QC USB key and Digital certificates)

• Not just about Technology - what about governance?
  – How do you get stakeholders to agree on;
    • Common definitions Trust &Security Models
    • Common Business Requirements &Specifications
    • Accountability and transparency mechanisms
    • What are business drivers ?
      – stakeholders need to integrate and implement Interoperability enablers