Privacy and Security within an Interoperable EHR

Stan Ratajczak
Director Privacy and Security
Solutions Architecture Group
November 30, 2005

Electronic Health Information and Privacy Conference
Ottawa Congress Center

Agenda

- Introduction to Infoway and it’s privacy / security mandate
- The Privacy and Security Architecture initiative
- Key privacy and security challenges for an interoperable EHR
Canada’s Strategic Response to EHR Challenges

- F/P/T governments’ agreed to take a national approach that could:
  - Develop solutions that operate across organizations, clinical systems, & jurisdictions
  - Share risks and costs across a broad constituency
  - Collect and share best practices
  - Help establish and drive standards for interoperability
  - Provide platforms for National Public Health Surveillance systems
  - Increase the market size and hence private sector responsiveness

- Canada Health Infoway launched:
  - an independent, not-for-profit corporation,
  - equally accountable to 14 F/P/T governments
  - invests on a 75/25 basis with provinces & territories for eligible projects

A unique approach was adopted, based on collaboration across Canada’s healthcare jurisdictions

Canada Health Infoway

Mission
- To foster and accelerate the development and adoption of electronic health information systems with compatible standards and communications technologies on a pan-Canadian basis, with tangible benefits to Canadians. To build on existing initiatives and pursue collaborative relationships in pursuit of its mission

Goal
- To have an interoperable electronic health record in place across 50 percent of Canada (by population) by the end of 2009
Infoway’s Role – Strategic Investor

Infoway focuses on initial investment in a solution & its deployment. Our unique role is in providing strategic leadership.

- **Funder**: “Fund & ignore”
- **Strategic Investor**: “Invest, advise & monitor”
  - Invests with Partners
  - Involved in project planning
  - Monitors progress of projects and quality of deliverables
  - Gated funding manages risk
- **Intervener**: “Work alongside & take over if needed”
- **Developer**: “Write code & build modules”

Infoway is Not
- A Granting Agency
- A Venture Capital Fund
- A builder, direct implementer or holder of proprietary solutions
- And does not collect data

Tying it all together - Service Oriented Architecture

JURISDICTIONAL INFOSTRUCTURE

HIAL Provides standards-based message set for securely exchanging patient information

An interoperable EHR captures all key clinical data on one screen (role-based)
Privacy and Security

- Addressing privacy and security issues are key to the success of the EHR

- End users (patients, physicians, health facilities) must have confidence and trust that privacy and security are being adequately addressed

- 80% of Canadians rate EHRs as a strong improvement over paper records in terms of the effectiveness for all those involved in the health care system and for the system overall*

- 84% agree that timely and easy access to personal health information is integral to the provision of quality health care**

*EKOS survey of 2000 Canadians, 2003
**EKOS survey of 2500 Canadians, 2004

Infoway’s Privacy Mandate

- Infoway’s funding agreement requires it to:
  - “incorporate the protection of personal health information in its activities in accordance with applicable laws and privacy principles.”

- Infoway achieves this by:
  - ensuring that privacy and security are addressed in the projects it funds;
    - Infoway requires every project it supports to conduct a Privacy Impact assessment
      - PIAs are expected to describe how the system will function and how it will address privacy rules in place in the jurisdiction
      - This means that developers must consider privacy in all phases of a project, (design, development and deployment) not after the fact
Meeting Infoway’s Privacy and Security mandate

- Infoway achieves this by:
  - working to identify and leverage best practices for re-use across the country
    - Infoway’s pan-Canadian view means that if a project in Ontario is looking at technical privacy solutions we can support that work and ensure it is available to other jurisdictions
  - working to ensure that projects adopt an interoperable approach
    - Infoway has worked with technology and privacy experts across the country to develop:
      - A statement of privacy requirements for an interoperable EHR system
      - A privacy and security architecture

Overview of the Infoway Pan Canadian Privacy and Security Conceptual Architecture Project
The iEHR Privacy and Security Challenge! Sharing Personal Health Information

- Will you protect the privacy and confidentiality of PHI?
- Can we share information?
- Is authentication and authorisation reliable?
- Are you authorised to access PHI?
- Who are you? i.e. organisation and provider

Sharing of PHI

Why Do We Need a Privacy and Security Architecture?

- Trust in the interoperable EHR is based on the assumption that it is private and secure. This is fundamental to acceptance and adoption by governments, healthcare providers and the public.

- As Personal Health Information (PHI) is shared across disparate systems, privacy and security are no longer local issues therefore must be interoperable.

Infoway leadership

- Stakeholders expect the Infoway Blueprint to provide the vision of a privacy protective and secure interoperable EHR.
What is the Privacy and Security Architecture?

- It operationalises Pan Canadian Healthcare privacy obligations and best practices.
- The PSCA document provides a conceptual view of different privacy and security services and components in the EHRI and how they interact with one another to facilitate interoperability within and across jurisdictions.
- It is developed to be flexible – it allows jurisdictions to use those features that are consistent with local legislative requirements yet support minimum interoperability requirements.
- A comprehensive set of documents that will guide jurisdictions in the development or procurement and implementation of secure and privacy enhancing interoperable EHRs across Canada.

The Privacy and Security Architecture process

PHIPA
AB-HIA
MB-PHIA
Others...

Privacy Legislation

Legislative Obligations
Privacy Policies
Privacy & Security Requirements

Technology Architectures are Driven by privacy and security requirements

Conceptual Architecture
Logical Architecture
Detailed Architecture

Privacy protective & secure HealthCare Solutions
Project Methodology

- The Pan Canadian Privacy and security architecture is based on:
  - The following sources of guiding principles
    - Canadian CSA Privacy Model Code
    - Internationally recognized Information Security Management standards
    - ACIET Pan Canadian Privacy and Confidentiality Framework
  - A clear articulation of business and legislative requirements based on a Pan Canadian privacy legislative scan
    - Identifies Pan Canadian privacy and security obligations
  - Development of Pan Canadian privacy and security requirements for an interoperable EHR
  - Consultative process
    - Multi disciplinary group of over 80 privacy and security experts, including National Provider Associations and vendors where consulted and provided invaluable input
    - 3 stage consultation process; Requirements validation, Architecture validation and a final revision cycle

Privacy Requirements – Organizing Framework

Privacy Framework

- The privacy requirements for an interoperable EHR are organized according to the 10 privacy principles of the Canadian Standards Association’s Model Code for the Protection of Personal Information (CAN/CSA-Q830-96)
  - The Code was published in March 1996 as a national standard for Canada
  - The 10 core principles in the CSA Model Code facilitate an easily recognisable, principled approach to data protection in an EHR environment

Security framework

- The security requirements for an interoperable EHR are organized according to ISO/IEC 17799-1:2000 Code of Practice for Information Security Management
  - The ISO 17799 Code of Practice is a widely adopted international standard for information security management
Objectives of the P&S Requirements Document

- To identify the Privacy and Security business requirements for an interoperable EHR

- Comprehensive set of requirements including policy, administrative and technology aspects

- Provide rationale for each requirement

- To contribute to the identification of the Privacy and Security services necessary to implement an interoperable EHR

Key Features of the privacy and security architecture
Key Features of the PSA

1. **JURISDICTIONAL INFOSTRUCTURE**
   - **Registries Data & Services**
     - Client Registry
     - Provider Registry
     - Location Registry
     - Terminology Registry
   - **EHR Data & Services**
     - Shared Health Record
     - Drug Information
     - Diagnostic Imaging
     - Laboratory
   - **HIAL**
     - Communication Bus
     - **Patient Info**
       - Patient History
       - Drug Profile
       - Laboratory
       - Diagnostic Imaging
     - **EMR**

2. **Key Features – To Access Personal Health Information**

   1. **PHI is to be only accessed by authorized Healthcare providers**
      - Provision for jurisdictional or regional access control rules applied in a consistent manner
      - i.e. Psychiatric information may not be available to the GP
      - i.e. Radiology reports not available to the ADT clerk
   2. **Patients have the right to determine the purpose, when and who can access their PHI**
      - Where applicable by law, PHI is only made available to a Healthcare provider if the appropriate jurisdictional and/or patient derived privacy rules are satisfied
      - i.e. Patient consent or masked data
   3. **Prevent unauthorized access to PHI**
      - The use of encryption technologies to protect against unauthorized access (confidentiality and Integrity) to PHI whether in storage or during transmission
Key Features –
The Right Information to the Right Person

4. Ensure that Healthcare providers are uniquely identified, authenticated and authorized to access PHI in a trustworthy common manner notwithstanding where they access PHI
   - Single sign on with one electronic credential (ID) recognised by all applications (Federated ID is the goal)
   - Defining and applying standardized predefined roles across disparate healthcare applications
   - Creation and validation for Digital Signature on electronic documents, i.e. ePrescribing, proof of authoring of, and acceptance of reports
   - Audit Trace – required for consent override and access: a fundamental privacy requirement – who, what, when, why has accessed PHI

Key Features –
PHI Is Accessed at the Right Time - in the Right Context

5. Information not typically available can be accessed in emergency situations
   - Support for predefined conditions for overriding privacy and access control rules
   - Support for extensive audit traceability in cases of exception

6. Concerns about the privacy risks of centralized data bases
   - Highly secure data centres
   - Federated data bases such that not all of a person’s data is within one database or in one data centre
   - Encrypt all PHI data
   - Privacy protective backup, namely encrypted
   - Use mechanisms to allow for de-identification and re-identification of PHI
How Will the PSA Help Infoway Stakeholders?

- It provides a vision of how iEHR systems can be developed to meeting the demanding requirements of sharing PHI in the health care sector while respecting privacy, confidentiality and security
  - Information must be shared immediately and accurately among a range of health care providers for the benefit of the individual yet remain secure and confidential
- It provides a roadmap for stakeholders during product procurement, system design, development, implementation and operation of interoperable EHR solutions
- Used while performing Privacy Impact Assessments
- Provides guidance to the vendor community to ensure they design privacy and security solutions for an interoperable EHR
Key privacy and security challenges for an interoperable EHR

Key Privacy and Security Challenges – Operational Governance of an iEHR

- Funding & operations of governance entities
- Definition of common Governance frameworks & models
- Rules for accreditation and conformance
- Definition of shared accountability Framework
- Definition of liability and dispute resolution mechanisms
- Definition of operational privacy and security standards
- Definition of risk management framework PIA, TRA
- Rules for accreditation and conformance
- Definition of common governance frameworks & models
- Funding & operations of governance entities
- Definition of shared accountability Framework
- Definition of liability and dispute resolution mechanisms
- Definition of operational privacy and security standards
- Definition of risk management framework PIA, TRA
- Rules for accreditation and conformance
- Funding & operations of governance entities
- Definition of shared accountability Framework
- Definition of liability and dispute resolution mechanisms
- Definition of operational privacy and security standards
- Definition of risk management framework PIA, TRA
- Rules for accreditation and conformance
- Funding & operations of governance entities
- Definition of shared accountability Framework
- Definition of liability and dispute resolution mechanisms
- Definition of operational privacy and security standards
- Definition of risk management framework PIA, TRA
- Rules for accreditation and conformance
- Funding & operations of governance entities
- Definition of shared accountability Framework
- Definition of liability and dispute resolution mechanisms
- Definition of operational privacy and security standards
- Definition of risk management framework PIA, TRA
- Rules for accreditation and conformance
- Funding & operations of governance entities
- Definition of shared accountability Framework
- Definition of liability and dispute resolution mechanisms
- Definition of operational privacy and security standards
- Definition of risk management framework PIA, TRA
- Rules for accreditation and conformance
- Funding & operations of governance entities
- Definition of shared accountability Framework
- Definition of liability and dispute resolution mechanisms
- Definition of operational privacy and security standards
- Definition of risk management framework PIA, TRA
- Rules for accreditation and conformance
- Funding & operations of governance entities
- Definition of shared accountability Framework
- Definition of liability and dispute resolution mechanisms
- Definition of operational privacy and security standards
- Definition of risk management framework PIA, TRA
Key privacy and security Challenges – Interoperability privacy and security standards

Privacy and security messaging standards

- Facilitate & support the development of privacy and security messaging standards for; authentication, access control, consent directive management
- Required to support interoperability of privacy and security functions across disparate systems and technologies.
- Increase adoption by the vendor community
- Facilitate the implementation of consistent level of privacy and security within The EHRS

Key privacy and security Challenges – Interoperability privacy and security standards

Privacy and security messaging standards

- EHRI Generic Communication Interface (focused on wrappers and protocols):
  - Security Management & Communication Interface
- Interoperable EHR Program - Privacy and Security Messaging Standards
  - EHRI Application Identification, authentication and authorisation
  - EHRI POS Application Identification, authentication and authorisation
  - EHRI User Identification, authentication and authorisation
  - EHRI User Role and rights management
  - EHRI Client Consent Directive (flag- metadata)
  - EHRI Check Consent Directive
  - EHRI Provider Digital Signature
  - Privacy Taxonomy (protected ID mapping)
Thank You

Questions?

Main website
www.infoway-inforoute.ca

Knowledgeway
http://knowledge.infoway-inforoute.ca/

Forums
http://forums.infoway-inforoute.ca

E-mail: sratajczak@infoway-inforoute.ca