Canada Health Infoway | Inforoute Santé du Canada

Privacy & Security Requirements: from EHRs to PHRs

Oct 28, 2010

Presented by André Carrington, P.Eng, CISSP, CISM, CISA, CIPP/C
Director, Implementation, Privacy & Security, SPS

Purpose

As suggested by this seminar's organizers, the purpose of this presentation is to assist Ontario stakeholders (eHO, LHINs, etc) with informative (not normative) guidance, regarding the development, harmonization and/or maintenance of Privacy & Security (P&S) requirements, via resources, context, considerations and lessons learned.

Agenda

- Security vs. privacy
- Requirements
- EHRS blueprint requirements structure
- Example requirements
- EHRS blueprint scope
- Lessons learned, managing requirements
- Other sources of requirements
- Portal and PHR requirements

Information security vs. privacy

- Information security & privacy have **similar organizational objectives**
  - to manage risk and meet due care; and
  - to enable appropriate use and collaboration.

- That said, privacy pertains to ***personal information and the law;***

- whereas security pertains to ***any asset,*** and has few explicit or specific legal obligations (due care is implicit).

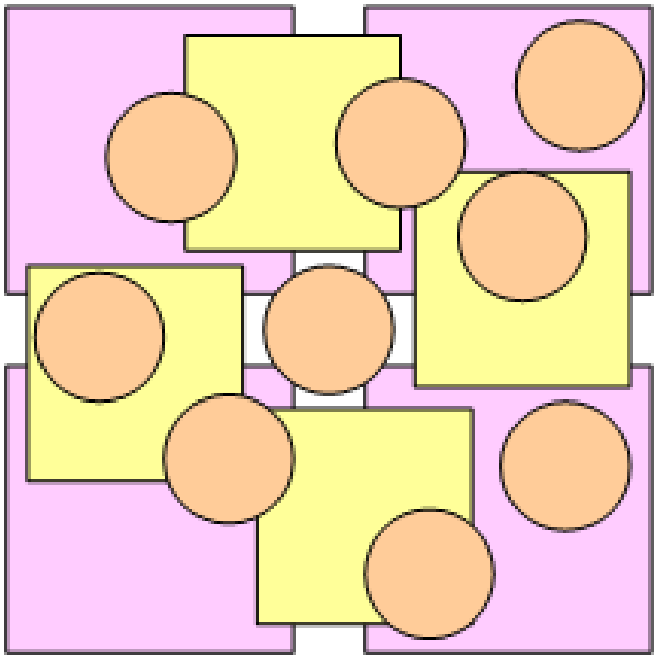
Information security vs. privacy

- To be more specific, privacy pertains to the collection, use and disclosure of personal information
  - with individual rights and organizational obligations set in federal, provincial and territorial laws

- Security pertains to the confidentiality, integrity and availability of any asset
  - with implicit due care obligations
  - with general requirements re the "safeguards" privacy principle
  - with a few specific requirements in privacy laws and privacy commissioner/ombud orders

Requirements

- All requirements should trace back to business requirements
- Technical requirements may not trace back to functional requirements



Business Requirements

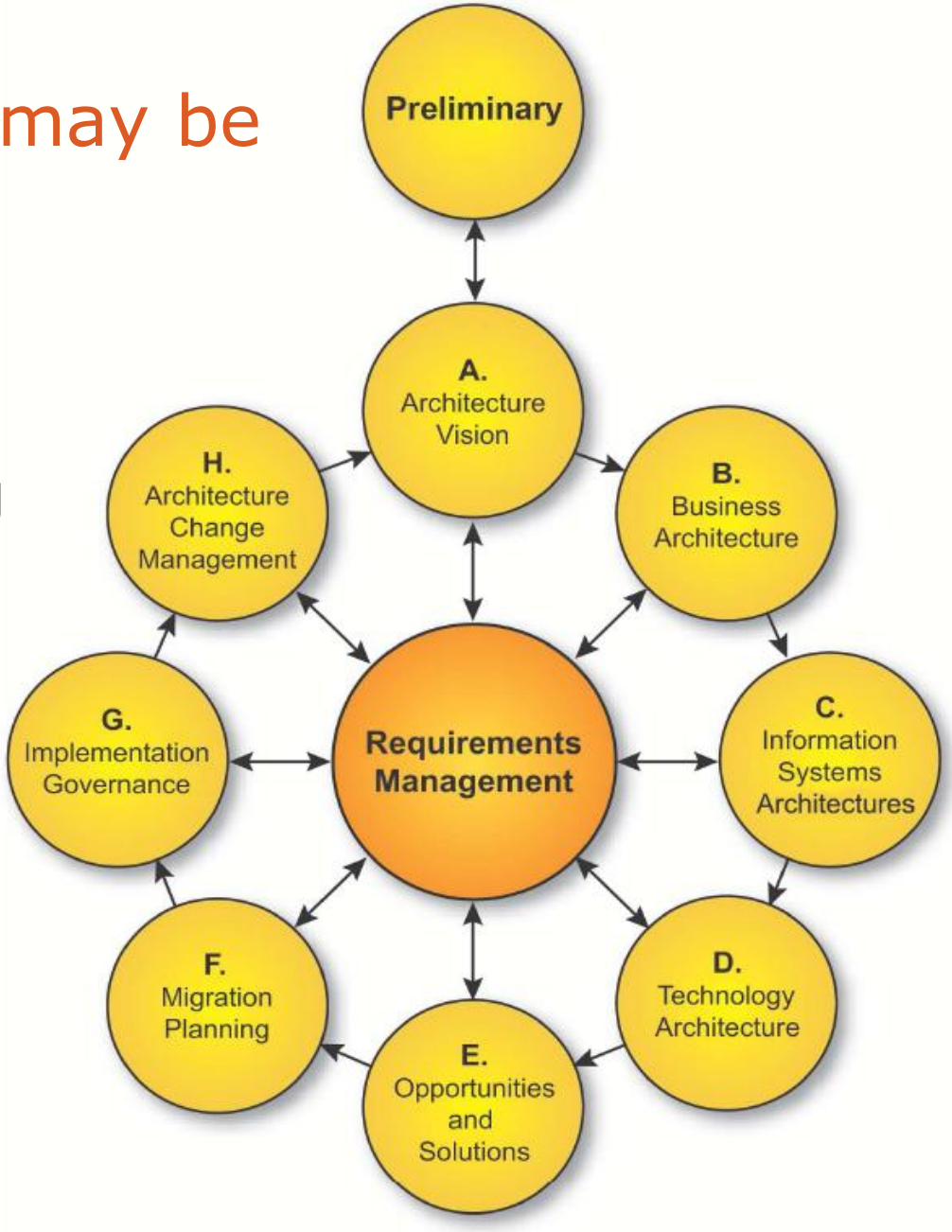
Functional Requirements

Technical Requirements

Diagram based on concept from Accenture Methods

Requirements may be created

- iteratively, complimenting and/or refining requirements from prior steps



Source: TOGAF

"EHRS Blueprint (v2) P&S Requirements"

The EHRS Blueprint Privacy & Security Requirements are ***identified*** as pertaining to:

- the EHR infostructure (EHRi)
- Point of Service (POS) systems connected to the EHRi
- organizations hosting components of the EHRi
- organizations connecting to the EHRi

Technical

Administrative

This allows people in different roles to focus on their respective areas.

…but they aren't ***organized*** this way…

"EHRS Blueprint (v2) P&S Requirements^"

are ***organized*** in accordance with the best practices they are based on:

- CAN/CSA-Q830-96 Model Code for the Protection of Personal Information (incorporated into PIPEDA)
  - 10 principles (28 blueprint privacy requirements)
- ISO 17799:2005* Code of Practice for Information Security Management
  - 11 control objectives (86 blueprint security requirements)

*this standard was re-designated as ISO/IEC 27002:2008 ; and it is complimented by ISO 27799:2009.

^ http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security-Requirements.pdf

The privacy code

CAN/CSA-Q830-96 Model Code for the Protection of Personal Information (incorporated into PIPEDA^)

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

^ http://laws.justice.gc.ca/eng/P-8.6/page-4.html#anchorsc:1

The security code of practice

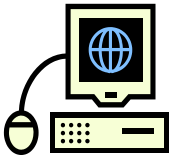
ISO 17799:2005* Code of Practice for Information Security Management

- Security policy
- Organising information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operational management
- Access control
- Information systems acquisition, development and maintenance
- Security incident management
- Business continuity management
- Compliance

*this standard was re-designated as ISO/IEC 27002:2005; and it is complimented by ISO 27799:2009.

http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS%2fISO%2fIEC+27002-2005

Example requirements



PR19: Logging Access, Modification and Disclosure

- The EHRi and POS systems connected to the EHRi must:
  - have a mechanism to record every access, modification or disclosure of ***PHI***, together with the time and identity of the accessing user;
  - have a mechanism to record every access, modification or disclosure of ***provider and user registration data***, together with the time and identity of the accessing user; and
  - where required by law, have mechanisms to alert the organisation's individual accountable for privacy…when ***[a breach of PHI is suspected]***

^ http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security-Requirements.pdf

Example requirements

Admin Requirement

SR5: Assessing Threats and Risks from Third Parties

- Organisations hosting components of the EHRi must ***assess***, by means of threat and risk analysis, the risks associated with ***access*** by external parties ***to hosted components or to facilities*** managed by external parties and must implement appropriate security controls where necessary to mitigate identified risks.

SR17: Terminating User Access When Terminating Employment

- All organisations hosting components of the EHRi or connecting to the EHRi must, as soon as possible, ***terminate*** the user ***access*** privileges of each permanent or temporary employee or third-party contractor who is a registered user of a ***POS*** connected to the EHRi or who has access to hosted components of the ***EHRi*** upon termination of their employment with the organisation.

EHRS blueprint v2 scope

- Focus:
  - Interoperability EHR/POS, inter/intra EHR
  - EHR services & infostructure

- Out of scope :
  - most network security
  - most logical design*
  - detailed design
  - some operations – e.g. server hardening
  - portals, PHRs, data warehouses, research, genomic databanks

*except some requirements and use cases at the logical level

other links: http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf
http://forums.infoway-inforoute.ca/PSA/PSA_Materials/EHR%20P%26S%20Use%20Cases/
http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf

Agenda checkpoint

- Security vs. privacy
- Requirements
- EHRS blueprint requirements structure
- Example requirements
- EHRS blueprint scope
- Lessons learned, managing requirements
- Other sources of requirements
- Portal and PHR requirements

How do we foster stakeholder agreement on common requirements?

- Understand stakeholders and their business drivers, opportunities, constraints
- Critical path
- The need to start now
- The need to be inclusive of future participants
- Pay attention to change management (tone at the top, heart of change – champions, mavens)

Be a pragmatist, not a purist (look for options)

- Seek agreement on higher-level principles first vs. detailed requirements, to avoid getting stuck
- Don’t worry about strict adherence to a method such as TOGAF.
- Disagreement about requirements, may be a timing issue re budget, availability of resources…
  - seek agreement on the roadmap, the process, the levels and even exceptions.
  - use formal governance!

Case study: Quebec

- Legislation and regulations provide the ministry with a role
  - responsible for the development and evolution of P&S requirements across the province;
  - to create (as a facilitator) the mechanisms whereby the regional authorities can achieve consensus on a uniform level of P&S requirements/controls
- The required activity also met regional needs for P&S requirement management
- Cost savings re development; competition for annual assessment

Case study: Quebec (continued)

- The Ministry asks that every healthcare facility submit an annual compliance report to the requirements
- Self-assessments are submitted to a portal on the internal network
- Followed by corresponding paperwork, proof, letter of attestation (incl. exceptions and action plan)
- The Ministry can see the provincial security posture

Case study: TLI specification crypto update

- The spec must facilitate interoperability
- The spec must support algorithms and approaches that avoid undue risk, and meet requirements
- Each jurisdiction has their own roadmap to meet TLI

- CSEC and NIST have deprecated the use of lesser encryption key lengths and weaker algorithms
- Rather than deprecate in TLI (future versions may):
  - In general, TLS clients and TLS servers negotiate the strongest mutually shared ciphersuite
  - For implementations that meet the spec, the spec requires support for sufficient algorithms, which are then used ***by default***, except for legacy systems

http://forums.infoway-inforoute.ca/webx?14@785.HKKJaQSpEkE.190@.ef3665d

http://forums.infoway-inforoute.ca/PSCWG/Work%20program%20and%20discussion%20documents/TLI%20Specification/TLI%20Crypto%20Update%20v1.01%20AC%2020101020.pptx

Agenda checkpoint

- Security vs. privacy
- Requirements
- EHRS blueprint requirements structure
- Example requirements
- EHRS blueprint scope
- Lessons learned, managing requirements
- Other sources of requirements
- Portal and PHR requirements

"P&S Resources and Standards" spreadsheet

- Architecture
- Information & IT Governance
- Processes
- Implementation

Microsoft Office
:el 97-2003 Worksh

http://forums.infoway-inforoute.ca/PSCWG/Meetings%20%26%20Administration/Fall%202010%20Infoway%20Partnership%20Conference%20Nov%2015%20-%2017%2C%202010

CHI "Information Governance White Paper"

Provider and Community Rights

- **Respecting communities of interest**
- UserId management and protection

Trust and Accountability

- Accountability
- Information custodianship
- Openness
- **Trans-border and cross-jurisdictional data flow**

Assessment and Compliance

- **Assessment of governance**
- **Compliance mechanisms**
- **Liability and sanctions**
- Risk assessment

Patient Privacy Rights

- Access to information
- Information consent
- Information notices
- Limiting collection
- Limiting disclosure and privacy protection
- Secondary use

Quality

- **Data retention**
- Archiving and disposal
- **Accuracy and data quality**

Safeguards

- Access controls
- **Electronic (digital) signatures**
- **Auditing and incident handling**

http://www.infoway-inforoute.ca/Admin/Upload/Dev/Document/Information%20Governance%20Paper%20Final_20070328_EN.pdf

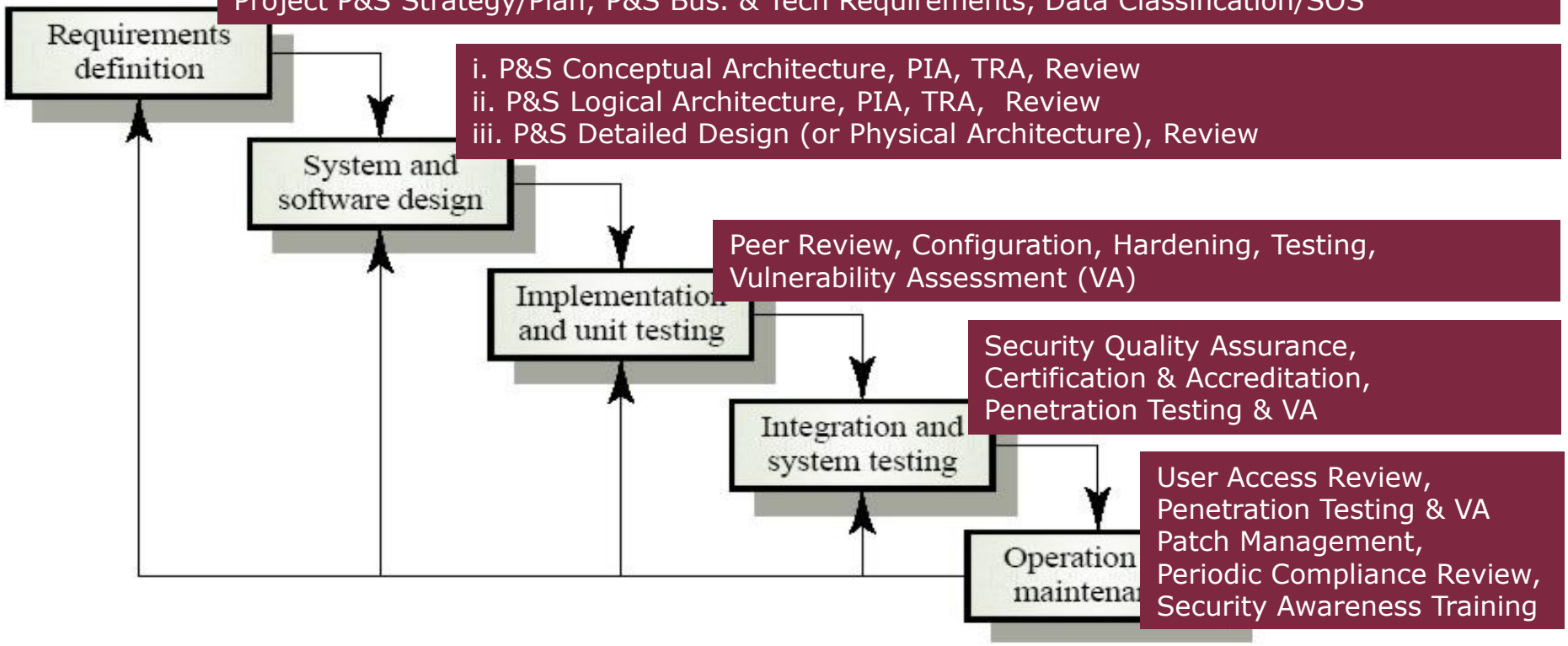
P&S requirements in processes

Governance P&S Activities and Deliverables

Laws, Regulations, Commissioner Orders, Principles, Policy, Strategy/Budget/Plans, MOUs/Contracts/SLAs/ DSAs/ISAs, Risk Management, Committees/WGs, REBs/IRBs, Roles & Responsibilities, Enterprise Architecture, Business Continuity & Disaster Recovery, Change & Release Management, Standards, Procedures

Project P&S Activities and Deliverables

Project P&S Strategy/Plan, P&S Bus. & Tech Requirements, Data Classification/SOS



i. P&S Conceptual Architecture, PIA, TRA, Review
ii. P&S Logical Architecture, PIA, TRA, Review
iii. P&S Detailed Design (or Physical Architecture), Review

Peer Review, Configuration, Hardening, Testing, Vulnerability Assessment (VA)

Security Quality Assurance, Certification & Accreditation, Penetration Testing & VA

User Access Review, Penetration Testing & VA Patch Management, Periodic Compliance Review, Security Awareness Training

Base diagram from ISO 12207 Software Life Cycle - Waterfall Model
Diagram concept by Andre Carrington

Recently published resources to consider

- COACH Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records
- Infoway's TLI Specification 3.0
- HL7 PASS Audit domain analysis model
- HL7 EHR-S Functional Model
- ISO DTS 14265 Classification of Purposes for PHI
- ONCHIT Draft Model PHR Privacy Notice

http://hssp-security.wikispaces.com/PASS_Audit
http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__model_phr_privacy_notice/1176

Upcoming resources

- Aligning Jurisdictional EMR specifications to Infoway EMR (interoperability) specifications
- Health Information Privacy (HIP) group's Common Understandings paper
- ISO/IEC 29101.5 Privacy Reference Architecture
- HL7 PHR Functional Model
- ISO/IEC 29100.3 Privacy Framework

Personal Health Record (PHR)

An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

The National Alliance for Health Information Technology: Defining Key Health Information Technology Terms, April 28, 2008

Typical P&S requirements in portals & PHRs

- Identity management capacity for large populations
- Consumer enrolment & authentication
- User agreements
- Privacy policies & statements/PIAs
- Browser privacy & security
- Server privacy & security
- Network security, penetration testing, audits
- Privacy protective e-mail notifications

Interesting privacy considerations in PHRs

- Consumer as custodian; provider is "hands-off"
- Consumer can impact privacy of third-parties
- Consumer understanding of privacy impacts re:
  - sharing data with other users
  - granting write access vs. custodianship
  - sharing data with applications (esp. external)
- Potential unmediated consumer access to EHR data
- Consumer experience with PHRs may set expectations for EHRs re: consent granularity, use & disclosure reports, EHR export, research opt in/out
- Data retention after account closed
- Ongoing visibility of erroneous/corrected data

Interesting security considerations in PHRs

- PHR process of on-boarding the EHR and applications: requirements, agreements, processes
- EHR/PHR account connection/enrolment
- Authentication per Windows Live ID & Open ID
- Direct access by EHR/EMR to PHR, to correct data
- Security of data sharing invitations
- Secure e-mail

Canada Health Infoway
Inforoute Santé du Canada

acarrington@infoway-inforoute.ca

Presented by André Carrington, P.Eng, CISSP, CISM, CISA, CIPP/C
Director, Implementation, Privacy & Security, SPS