Concepts for a standard based cross-organizational information security management system in the context of a nationwide EHR

Alexander Mense
University of Applied Sciences Technikum Wien

MedInfo 2013
August 23rd, 2013
Health data processing evolution …
Austria‘s national EHR (ELGA)

- Standards based (IHE, HL7, LOINC, DICOM, LOINC, …)
- Patient controls access
- ELGA GmbH responsible organizations to set up ELGA
Health data and security & privacy

- Health data = sensitive Data => requirement for security & privacy
- Information Security is the basis for privacy
  - CIA triad (Confidentiality, Integrity, Availability)
- Information Security
  - is not only „technical thing“ - requires a combination of technical AND organizational measures – needs “holistic” approach
  - is complex
  - Requirements constantly change
… security requirements evolution …
Sharing Health Information and Information Security

- Setting up networks of health information providers and consumers requires new security concepts for securely managing shared data.
- To ensure protection of health data in this context it is important to force a specific security level in all involved organizations (document providers / consumers, network service providers, core service providers).
- Every participating organization has to implement a certain security level based on a common security policy.
  - But each organization has to keep its own information security context (which is of course influenced by the overarching information security policy).
Requirement for Information Security Management

- Information Security always
  - ... needs to be proactive
  - ... is a risk management based permanent process
  - ... needs to be permanent checked and improved
  - ... needs to be **actively managed**

- Information security management systems (ISMS) are
  - an appropriate and approved tool for organizations to maintain information security
  - well known in many business areas
  - Usually based on the international ISO 27xxx standards
    - Provides also certification
    - In Austria even some hospital organizations are already certified
Security Management for sharing health information across many organizations

- Define security requirements and measures in contracts
  - P2P contracts are not manageable in large networks
  - Static contracts “one size fits all” are not enough

- Need for cross organizational Information Security Management / Information Security Management System (ISMS)
  - Should be based on international standards
  - Define and maintain an organizational framework to ensure an appropriate, agreed and sustainable security level for an multi-organizational (cross-organizational) information security context
First step

- Evaluate possible approaches by analyzing international standards and frameworks for their applicability or adaptability
  - ISO 27000 series (provide ISO 27799 for medical domain), BSI Standard (Germany), Payment Card Industry Data Security Standard (PCI), European Privacy Seal, COBIT
Not directly applicable

- All frameworks are scoped for a single organization
  - Besides PCI which doesn’t fit technically

- Further focus on question “is it possible to use ISO 27000 series in a cross-organizational setup”
  - Define core requirements for ISMS
  - Evaluate potential implementation scenarios
Core aspects of an ISMS

- **Defining a clear scope**
  - an ISMS needs a clear scope and requires a central Information Security Policy and an risk management process.

- **Responsibility of management**
  - the management plays a key role in the implementation of an ISMS (e.g. defining the information security policy, defines roles and responsibilities …).

- **Commitment of the organization**
  - the whole organization is committed to the goals, policies and processes within the ISMS
Core aspects of an ISMS

- **Organizational Roles**
  - Information Security Manager, IT-Security Officer, Risk Manager, Auditor and an ISM Team - well integrated into the organizational structures

- **Processes and documents**
  - clearly defined processes and set of policy documents describing Information Security Policy, Security Guidelines, classification of docs, processes for risk management and audit

- **Need for continual improvement**
  - ISMS is a management system that defines, implements, monitors and continuously improves measures for information security. E.g. based on Plan-Do-Check-Act model
The need for hierarchy

- All core elements can “easily” realized within a single organization but lack in a multi-organizational environment.
- Results in the need of an additional organizational layer – can be but must not be necessarily an organization.
Implementation core points

- Commitment of the organization
  - Can be implemented by a multilateral agreement / contract an organization agrees to and is deposited at a custodian

- Roles & Responsibilities
  - Important role of security manager can be fulfilled in cross-organizational setup by a security management team
    - Defines central documents as well as common methods and rules for the risk management process
  - Risk management has to be done by the management layer as well as every organization
  - Periodically audits are essential and have to be implemented at both layers
Implementations core points

- Security documents
  - Central information security policy as well as the security guideline is defined on the management layer by the IS-Management team
  - Each organization has to implement the security guidelines based on controls from ISO 27002 or ISO 27799
Conclusion & Challenges

- ISO 27xxx standards series can be used for information security management in a cross-organizational environment

- Selection of appropriate controls?
  - Individual responsibility of each organization
  - Selection based on the role of the organization
  - Baseline security as a basic requirement

- Dealing with “third parties” outside the security context?

- Maturity model for the implementation phase to classify an institution’s security level?
  - Big number of different organizations means different levels of progress in implementing security measures
Thanks for your attention!

alexander.mense@technikum-wien.at