IPS: Security Services For Healthcare Applications

Lorenzo D. Martino, Suchit Ahuja, Elisa Bertino

*Computer & Information Technology, Purdue University, USA 1Computer Science, Purdue University, USA

Background

• Need for longitudinal Electronic Health Record, but
  – Fragmented Systems
  – Interoperability and Standardization issues
• Federal initiative for Electronic Medical Record (EMR)
  – Enable sharing of medical data
  – Reduce healthcare information / administration costs
• Personal Health Record (PHR)
• Personal Health Applications (PHAs)
• Legal & Regulatory Compliance issues
  – HIPAA Security Rule & Privacy Rule
• Security and Privacy challenges

Personal Health Record (PHR)

• The Markle Foundation defines the PHR as an electronic application through which individuals can access, manage and share, their health information in a secure and confidential environment.

Personal Health Applications (PHAs)

• According to Project Health Design, Personal Health Applications (PHAs) are software tools that assist consumers to track and manage the health status and medical conditions of themselves and their families
• Provide a shared infrastructure to promote interoperability among healthcare applications


Examples: Microsoft HealthVault, Google HealthCare Initiative, etc.

Scenario

• PHR provided by third party vendor
• Several healthcare providers offer web-based PHRs to provide 24x7 accessibility for patients to their medical records
  – Limited functionality without sharing data with external entities
• Increasing demand for PHA modules to be integrated with PHRs to improve and increase functionality for patients
• PHR vendor & customer / patient - NOT HIPAA “covered entities”, but PHR vendor has to cater for LIABILITY due to privacy breach
• Patients want to control their data:
  – Patients “data ownership”
  – Patients define access control policy on their data

PHR System Design Security Challenges

• Usability: accommodation of patient-centric policy options
• Manageability by the PHR service provider
• Security and privacy: mediating between PHR service provider, patient and third parties security and privacy requirements and obligations

Process Flow

• Patient signs-up for PHR service and opts-in/opts-out default PHR vendor privacy policies
• The patient may modify the default policies and allow other subjects (family members, Primary Care Physician, Healthcare Providers, etc.) to access his PHR data. For caregivers, a notification and an e-consent process is activated
• PHR vendor privacy policies (and patients' modification thereof) defined according to a privacy-extended Access Control model
• Engineered process to define patient data structure and data privacy sensitivity:
  - standard-defined healthcare data categories by ASTM DHHS, CDA, etc. drive PHR data grouping, easing data exchange
  - Electronic Protected Health information EPHI as defined by HIPAA to identify privacy-sensitive data

Patient Privacy and Security Challenges

• Patient-centric Access Control Policy
  – Data Categories: Electronic Protected Health Information (EPHI) – HIPAA
  – Entities + Levels of Access
  – Purpose of Access
  – Access Time
• Integration of an e-Consent process into the overall workflow: Patient + Provider
  – Patient should be NOTIFIED of privacy norms, coverage and responsibility
• To provide patient with Access Control mechanisms in order to control access that can be easily understood and configured in the system
• Privacy-Aware Access Control based on purpose of access
• Authentication / Digital ID Mgmt. mechanisms for granting access to other entities according to patient-centric policy
• Over-riding the patient-centric policy during emergencies to provide access
  – “BREAK THE GLASS” principle

Security / Privacy as a Service

• Use of RBAC in heterogeneous eHealth systems
• Roles can be pre-defined and assigned specific pre-identification parameters. The challenge is to investigate possibility of Dynamic Role Creation based on RBAC
• Interoperability + Security & Privacy: Identity Mgmt., Authentication, Access Control

SOA approach to Security & Privacy

• Patient-centric & Policy-based security services
• Service Classes
  • Digital Identity Management Services
  • Authentication Management Services
• Service Classes and Auditing: Logging services for regulatory compliance