End-to-End Security for Personal Telehealth

Asim, M., Koster, P., Petkovic, M.
Healthcare Information Management, Philips Research Europe
Outline

• Introduction to Continua
• Continua E2E architecture
• Security in Continua 2010 specifications
• E2E security and privacy requirements
• Consent management in the Continua architecture
• Conclusions
Continua Health Alliance

Interoperable personal tele-health
Continua E2E Architecture
Security in Continua 2010 specification

- TLS confidentiality + integrity
- IHE XDM → S-MIME
- IHE ATNA auditability
- WS-I BSP → TLS v1.0 confidentiality + integrity
- WS-I BSP → WS-Security Header + SAML 2.0 authentication
- IHE ATNA auditability
- Zigbee security confidentiality + integrity
- Bluetooth security authentication + confidentiality
E2E security and privacy requirements

- **Identity management**
  - Unambiguously linking measurements to the patient
  - Interoperable protocols for identity linkage and cross-referencing

- **Integrity and data origin authentication**
  - Measurements are being taken in an uncontrolled environment
  - Authenticate data sources e.g. users and devices
  - Prevent or detect unauthorized data modification

- **Consent management**
  - Patient expectation? (Participation, accountability, specification of purpose, limits on data collection/use, transparency
  - Ability to specify and revoke consent preferences
  - Enforcement of patient consent along the care path
Design for the consent management at the HRN-IF

• Specification of consent

• Consent Directive as CDA document
  - Implementation Guide for HL7 CDA R2 Consent Directive

• Semantically interoperable

• Encoded using standard terminology

• Successor to the IHE BPPC (Basic Patient Privacy Consent) profile
Alice is presented with a default consent policy: Nurse@DMO may disclose her information to Dr. Bob for the purpose of treatment.
Consent Directive Analysis Model

- Consent specification
  - allow/disallow action
  - purpose of consent
  - effective period
  - additional conditions

- Action Specification
  - hierarchy of operations applied to information

- Health Information Affected
  - Related to a diagnosis
  - Data Sensitivity
  - Coverage Type
  - Type of information (e.g., results)

- Privacy Policy Reference
  - policyId: id
  - description: String

- Consent Directive
  - subjectOfConsent
  - receive

- Medical Record Reference
  - Patient Identification
  - Medical Record Identification

- Information Sender
  - Organization
  - Role
  - Identity

- Information Receiver
  - Role
  - Identity

- Action Specification
  - hierarchy of operations applied to information

- Consent Directive Analysis Model
Consent Directives Reference in CDA Doc

Table of Contents

- Allergies, Adverse Reactions, Alerts
- Medications
- Vital Signs
- Results
- Procedures
- Provider Orders

Allergies, Adverse Reactions, Alerts

<table>
<thead>
<tr>
<th>Substance</th>
<th>Reaction</th>
<th>Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penicillin</td>
<td>Hives</td>
<td></td>
</tr>
<tr>
<td>Aspirin</td>
<td>Wheezing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nausea</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>Active</td>
<td></td>
</tr>
</tbody>
</table>

Instructions
Design for the consent management at the HRN-IF

- Provide(Health Document, Patient Consent Document (optional))
- Query(Patient Consent Document)
- Query Response
- Retrieve(Patient Consent Document, Requestor Token)
- Response(Patient Consent Document)

Consent management at the HRN interface
Questions