Framework Model and Principles for trusted Information sharing in Pervasive Health

Pekka Ruotsalainen, Research professor
Adjunct Professor
THEWS Team: P. Nykänen, B. Blobel, A. Seppälä and H. Sorvari
Topics discussed
- A framework model for pervasive health
- Trust and privacy challenges
- Principles and rules for making pervasive health trusted
- Why new rules are needed?
- Remaining challenges
A Framework Model for Pervasive Health

We use a metaphor of linked digital domains or bubbles developed for ubiquitous environment and personal spaces. In our model:

- Each domain has **own** security and privacy rules and business needs
- **Pervasive health is a dynamic network** of domains which is created managed by the person (the Data Subject)
- **Health data** is collected, processed and disclosed **dynamically** between domains and for different purpose
Pervasive Health is different
- It takes part in open information space
- It uses ubiquitous computing
- It is not a part of today regulated healthcare
- Any kind of health data is collected and used
- Health data is not stored in EHRs
- The data subject (DS) is a person not a patient

(Source: Positionspapier der Arbeitsgruppe Telemedizin/Disease Management)

Wide range of contextual data is collected

(Source: B. Blobel)
Trust and privacy challenges – without new rules
- No predefined trust exists
- Data can be collected and processed invisible
- Difficult (or impossible) to control the use and sharing of data
- Lack of transparency and awareness in data processing
- Contextual information can be easily misused
- Dataveillance enables monitoring of person’s daily activities and behaviors
- The information space has unlimited memory.

In information space and privacy and information autonomy are main concerns.
## Updated principles and responsibilities for trusted pervasive health

<table>
<thead>
<tr>
<th>Principle</th>
<th>New principle or responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal privacy</td>
<td><strong>Right to define</strong> situation specific, context-aware and granular personal policies regulating the processing and disclosure of personal health data.</td>
</tr>
<tr>
<td>Withholdings</td>
<td>The <strong>DS has full control</strong> over the content of health data</td>
</tr>
<tr>
<td>Trusted usage</td>
<td>The <strong>DS can verify dynamically the level of trust</strong> of any domain. There is no need to accept blind trust.</td>
</tr>
<tr>
<td>Control over the collection, processing and dissemination</td>
<td>The <strong>DS have rights to control</strong> the use health information both inside bubbles and between them.</td>
</tr>
<tr>
<td></td>
<td>The DS shall have <strong>tools to control</strong> over the creation, collection, processing, storing and destroying of her personal wellness information.</td>
</tr>
<tr>
<td>Transparency</td>
<td>Systems have <strong>responsibilities</strong> to ensure transparency in data processing, openness of relationships between spaces, openness of their interests, policies and environmental and contextual features. Systems and stakeholders have the <strong>responsibility</strong> to publish necessary information for trust verification and transparency. The <strong>DS have right to be aware</strong> of all events and situations where health data is collected, processed, stored and shared.</td>
</tr>
</tbody>
</table>
In today healthcare:

- Leading concepts are information security and blind organizational trust
- Patients’ information autonomy is limited
- Health professionals control the content and use of healthcare data
- Both in processing and communication of health, there is lack of transparency and awareness

The use of today healthcare rules in pervasive health means that our daily life will be monitored and controlled

The use of our rules makes pervasive health trusted
Technical challenges

• Healthcare specific IT-technology is not needed. We can use solutions developed for social web and web of knowledge.
• Today IT-systems should developed to **support policies and awareness**
• **New services** for trust verification, policy conflict resolution and personal policy management are needed.
• New **data model** for health data is needed
• Common ontology for trust and security should be adapted

Main challenges are political

• Stakeholders (e.g. healthcare professionals ) should accept principles and responsibilities
• A common regulatory frame is needed
Trusted Pervasive Health is out of there

Thank you for listening  - e-mail: pekka.ruotsalainen@THL.fi