Information Modeling Project/FHIM Meeting

Summary of Call

Date/time of call: Friday, July 18, 2014 2:30 - 4:30 PM

Attendees

1. Steven Wagner
2. Alberto Llanes
3. Galen Mulrooney
4. Ioana Singureanu
5. Jackie Mulrooney
6. Kathleen Connor
7. Munir, Huma (DoD-DHA)
8. Stephen Hufnagel
9. Stevenson, Loren (VA)

Updates on S&I and FHA Initiatives *Steve Wagner*

* Observations of Tiger Team meetings was discussed. Consensus was that various models were being looked at with no firm decisions having yet been reached.
* Steven and Ioana discussed modeling being done with QUICK at S&I.
* Galen noted Data Provenance was pretty much starting "from scratch" although FHIM was asked to provide a field so various parts of the model could be pulled up by initiative relevance/map.

Other Business

* Value sets of OIDS for security labeling (HL7 Healthcare Privacy Security Classification Table.xlsx) were reviewed.

Modeling the Privacy and Security Domain *Galen Mulrooney*

* Started Security And Privacy Modeling using Rational Architect
* Decided to use ObligationCode, no longer using EventCode under BasicPolicy under Policy.
* Thinking was that consent constrains the policy class but the policy class is already constraining so not needed. Sensitivity is a characteristic of resource. Sensitivity is applied per "policy". Iona thinks that sensitivity should be assigned by the enterprise but when communicating between enterprises, sensitivity might not be handled the same way. Clearances need to have both the sensitivity and clearance levels sufficient to open the resource. Levels of assurance is also associated with identify spoofing, but its more than that, it includes clearances and trust-related data. Clearance must be sufficient to match the security label. Policy -> user can access the resource if they're trusted, and if and only if their clearance matches or exceeds the security label requirements. Purpose of use, obligation and refrain go together. Security label may contain a field for sensitivity.
* The SecurityPolicyInformation File contains the rules that are used to define the security labels for classifications. Usually this is somewhat static but could be changed between organizations. Basically says how security labels are constructed and the semantics of it. See http://www.isode.com/whitepapers/why-spif.html
* The SensitivityLabelAssignmentPolicy defines how the sensitivity is set.
* Galen to look at the Healthcare Classification System.
* Provenance policies will vary by organization and will describe how much to trust resources with different provenance. Some of the security label is computed based on the provenance. In UML this might be a derivation relationship. They policy need to be brought into the decision making of the PDP while the provenance is in the resource.
* Question: Is there a value set out there for provenance now?
* Answer: There is, a valueset in the HCS security label vocabulary, there's entries for who reported it, who recorded it, etc.

Next Meeting: Friday, July 25, 2014 at 2:30 EDT

| Action Item Description | Responsible Individual | Due Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Information for future FHIM information and terminology modeling calls:

1) Information Modeling (IM) project call (Every Friday)

Time of Call: 2:30 to 4:30 PM Eastern Time

Dial-in Information: 1 (773) 897-3018, Access Code: 585-151-437

Web Meeting URL: <https://global.gotomeeting.com/meeting/join/585151437>

2) Terminology Modeling calls (Every Wednesday)

Time of Call: 2:00 to 3:30 PM Eastern Time

Dial-in Information: 1 1 (773) 945-1031 Access Code: 849-124-653

Web Meeting URL: <https://global.gotomeeting.com/join/849124653>