# Meeting/Call Notes Open HIE IL Community Call 4 March 2014

**Meeting purpose:** Community Call for OpenHIE IL Community

**Attendees:**

Linda Taylor

    Joan Africa Brown

    Derek Ritz

    Larry Lemmon

    Shahid Khokhar

**Agenda:**

* **Vision, Mission (RC) and Values progress (LT)**
* **CSIR team involvement**
* **Discussion of security workflows**
* [**https://wiki.ohie.org/display/documents/Common+message+security+workflow**](https://wiki.ohie.org/display/documents/Common+message+security+workflow)
* **Call time - changes to 10am (EDT) from next week ( remains 2 pm GMT/UTC)**

**DRAFT 2 - ONE TEXT**

**Vision**

**·** A world in which the exchange of health information improves health outcomes in low to middle income countries.

 {The present overarching OHIE vision (from the web page) is:

*We envision a world where all countries are empowered to pragmatically implement sustainable health information sharing architectures that measurably improve health outcomes.}*

**Mission**

**·** To develop an open community to *discuss the challenges around interoperability in health information systems, as well as to design an architecture and develop a reference application to enable easier interoperability between disparate health systems and components*. We promote the use of appropriate standards to support best practices for health data exchange.

**Values**

**·** We hold the requirements of our target community of  users as our primary concern

·         We are an open and collaborative community, valuing the inputs and respecting the contributions of every member

·         We strive for elegantly simple solutions to complex problems

·          We aim for ease of use to reduce barriers to adoption in low-resource settings

           We are implementation-driven in our designs and requirements, valuing practical solutions to real problems and real needs

**Meeting Notes**

**83837901 recording available on line here for 30 days**

[**http://www.conferenceplayback.com/stream/48682448/83837901.mp3**](http://www.conferenceplayback.com/stream/48682448/83837901.mp3)

**Vision Mission and Values**

LT: thanks for comments received for the Interoperability Layer draft. Not much feedback was received.

Comments from SHR also incorporated where relevant. Latest text is above

Highlight two things: Making sure that our vision harmonises with the overarching OHIE vision.

LT: need to define what an open community is. Need to be more descriptive on how we work and what we mean by that term

Any comments on the process thus far.

DR: Process of one write works well.

LT: will take text that we have now for a second round of comments from community members

LT: Do we need to be more descriptive around what an open community is

DR: there is lots around what the open community means on the base site which should be enough information.

LT: This process will continue and the document will be sent out tomorrow.

**CSIR**

LT: Jembi team members Carl, Ryan, Hannes, Dominic and Pierre are in Pretoria at CSIR which is the Council for Science and Industrial Research in South Africa. Excited about getting them involved.

Working currently on a hackathon on the Node JS version of the HIM. They are a strategic partner and we are hoping to get them more involved in this community.

DR: CSIR folk looking forward to being involved with us around these technologies including the IL

LL: what other areas will they be interested in understand the IL

LT: Background to the involvement is the initiative to establish a National Pregnancy Register in SA. Currently the aim is to register women who are pregnant to start with and phase two would be to send standardised messages to these women. Chris has been involved in developing the architecture around that. We are seeing the first implementation of this initiative, this hackathon is the first step in showing that the technology can work.

We are working with the ICT focus unit Meraka Institute.

DR: CSIR are becoming a centre of excellence, have been tasked by SA Govt with developing the eHealth National Standard Framework. The framework is not yet public but this project is the first part of following this framework.

They still have a national Enterprise Architecture Project underway but this is pre-adopting some of the work items that are internal still but they are making use of it

LL: think it is good.

DR: it’s a bit of a thin edge of the wedge and that is what is exciting about it

**Security Workflow**

LT: Indicated that RC did a sequence diagram that is available to team members on the wiki link above.

DR: 3 elements RC has identified as part of IL are a core, role based access control and an orchestrator.

DR: not sure we are clear yet what is inside the IL vs what is something else. We may struggle with this. One reason is a Natural tendency to want to stop scope creep. The other thing creating tension is the whole of the HIE infrastructure should be one single thing being seen at the POS. It is just something that is exposing interfaces at the bottom, for us in a clear box it is what the IL does.

Many things need to be done from the point of message management when something is sent from POS to the HIE. Will be challenging to say when the IL hands off to some external service that we also have a boundary around. We started to find this when we spoke because the folk in the facility register had already made some progress on this and had as part of the facility register some services they were using were being externalised, so we thought everyone should use those so we put them into the IL, that's turning the IL into what is inside its envelope as the place where all of the shared services are, it will create scope creep.

Diagram identifies 3 bits but they are not the only moving bits inside the IL. Do we have a diagram that shows all these moving bits that we are considering to be part of the shared envelope?

LT: the only documents we have are the high level ones on the wiki, this is the first point of trying to define what the other pieces are

DR: so we are including the mutual authentication to be inside the core? LT: Yes DR: Fair enough they are all transport related stuff mainly we are making use of the transport layer stack at that point. Everybody feel that it is TLS, looking at message 7.

LL: can we equate with these items what will be Node JS and what will be strictly the mule or core

LT: in this diagram the IL core and authentication control would be NodeJS and the orcherstator sits outside that

SK: seems like authenticating to any registry goes through the IL Core. in the past we talked about connecting to the registries directly as well. Is that not the case anymore or will everything go through the IL?

LT: discussions involved at in Jembi the default is to go through the core even if it is just a pass through channel but to keep the pattern

SK: not sure if a decision has been made on that

DR: recollection from architecture mtg Indi. Central service managed by the IL that we use openID to do authentication. And it seems to be going through an authority step but it doesn't look like it is following a registry workflow. Looks like it is a registry maintenance workflow, something to use not only to fetch something from a shared health record but maybe update something in a health worker or provider or a facility registry

LT: think it is intended as a generic workflow

DR: Step nine tells if it is somtheing straightforward then we can tell at nine that access should be granted. Based on a header level inspection vs a disassemble message approach.

DR: at message 10 the core is handing over to the message orchestrator, it is up to you now. at message 11 the orchestrator does a deep inspection of the message, 12 assumes it is a two way arrow because it never hears back from the RBAC, 12 is saying I submitted to the RBAC using one message approach there should now be a message from the orchestrator to say what the result is. Then we get a message back from the core that received no communication so not able to know if it must return true or not, may be a mistake that the response should be the reply to 12 from the RBAC. 13 should be the reply to 12.

DR: 14 and 15 only happens if RBAC= true another alt box around 14 and 15 if RBAC=true

DR: not what we were talking about at Indi, there was more within the discussion that if we are able to set up central authentication service for registry management, that is going to be a very light traffic use case, that we could allow authenticated users to have direct access and that the registry application, all will have some sort of web based management UI that the centralised authentication would allow the UI to know who it is talking to and let them know what that person is allowed to do.

DR: pattern shown here is pushing into the IL things that it is going to have to know from each of the registries on who can do updates, deletes and read only with relaxed permission while the others quite strict. Difficult to push all this application logic back into the IL. And that was the gist of the argument being made by the registry folk that it would know who the people are who are allowed to do these things and it was part of its allocation logic like the resource mapper is an application not just a registry

This will require the application logic to be in the RBAC, it makes the registries just be registries

Our challenge is that our registries are applications more than registries.

LT: what about the use case when the registry is just a registry?

DR: our challenge is going to be that in terms registry maintenance is not always part of the covering of the IHE we are not able to do registry maintenance. Aware of HL7 that does that in Canada they have not included the registry maintenance in their version of an HIE/HIEL. Ed was advocating for a central way just to say who this is and once the unknown has proved who they are the system can do what that person is allowed to do on the resource mapper and then manage what the person can do on the application. That could lighten what could be an onerous user profile permissions job inside the RBAC

Focus on the use of the RBAC for the maelstrom of providing medical care. Facilities would only be set up a few dozen for a year but at scale for any country they will be doing a few dozen transactions per minute in their IL. Think it would be better to use the RBAC in terms of which PHI records is this user allowed to see what shared health record to determine what SHR content the person can see, to take into account privacy laws in each country. Rather than the onerous job of which user is allowed to update the operating hours of a facility and the difference in traffic is two to three orders of magnitude

SK: does that imply that the role base authentication should be outside of the IL

DR: have authentication in a simple way eg. If you're on the provider list you have access to the health records others more specific authentication if needed for who has access to the health records

DR: citizens could have control of who has access to their health record, could set up consent directives

DR: big switch approach in Canada a patient can opt in or opt out option set up a consent directive to decide who has control of who has access to their records. In Canada simple switch you can decide who has access to your records.

 Doable from both standpoints. Health sharing infrastructure must abide by the country health privacy laws

LL: where do we see the function happening

DR: role based access control at its simplest or consent directed. Have advocated for the RBAC approach

LL: where would the authority be to do the function?

DR: advocated for simple RBAC that you could put into the orchestrator. Need to have info from a couple of places. Likely that the orchestrator at step 11 inspect message content, probably involving a deep inspection who is doing the request, use health worker registry to establish attributes at 11.

Health registry comes back with a demographic for the person or we could check the patients’ record to see who can have access in the client register record. Flag could be used to see who has opted in and who not for access control

Look at combo of records to see if the provider is allowed and if the patient has allowed access to who can see their record

DR: easier if it is in the RBAC engine the orchestrator does the transaction and fetches the information needed to do the authentication. In 12 pass the info to the RBAC and that becomes a programmable thing. Have the RBAC engine preserve the specific complexity and the orchestrator have that many if blocks. Each one optimised for what it is doing.

LL: trigger event is normally the check in to the visit to a service and OpenMRS starts a full dump of the patient information therefore will the restriction be in the SHR URL or in the POS at the request

DR: need to have a message that says it’s an event that triggers it, not just starting the process of a visit

LL: will we have trigger events from the POS to control a lot of the access, are we only going to rely on the role of the requester or that combined with a trigger event

DR: yes certain message types will be used as trigger events. Depends on the message logic type and the various whos, who is the requester and who is the subject of care.

DR: the RBAC would not be preprogrammed it would be based on the privacy policies of the country we would just give a place where that can be programmed

LL: more complicated than we have sketched.

DR: looks like it satisfies the requirements for handling those use cases

DR: need to have a realisation that there will be a lot of fetches at step 11 to get the consent information and to get the type info of the provider. Message type will be part of the inbound message of the POS. Useful to show that there are other fetches at this step. The orchestrator after fetching then passes all to the RBAC

RBAC does its conversation at 12 and 13, 14 and 15 have to be in an alt box only happen if true and if not true 16 and 17 return with a fault

DR: this pattern is more applicable for our repository rather than registry.

Facility registers person requested that a very centralised authentication would allow the registries do their own authorisation. Our focus should be how to do a really good job of RBAC rather than focusing on all the registry maintenance

Only support registry maintenance should be around adding and updating information in the client registry, given the maternal use case focus we currently have.

LT: diagram assumes that there is a client and facility register in place, whathappens when these are not available.

DR if only the IL you have no use case

LT: if you only had a repository as your simplest first implementation

DR: then the RBAC what would drive the logic would only be what is in the message.

LT: raise the issue again on the next call when the rest of the team is on the call.

DR: point out the only authentication is application level authentication doesn't look like the openID service and this does not look like the one discussed at the architecture meeting. A strong case made for central authentication service thatwill do web basedauthentication for those end users using web based application to manage underlying registries. Very specific around what resource mapper needed but also a clear consensus that, that as a pattern is what would be adopted more and more especially  as we get web based POS applications or hosted ASP based services applications. The capability to use centralised end user authentication is a useful service to start, we'd use it more going forward. The TLS is a certificate that is loaded on the service at the POS application server so that is authenticating an instance of OpenMRS it is not authenticating individual who's logged into the MRS.

DR: Advocate for that to be a separate IL box but that makes the current diagram more complicated.

DR: we need to identify that this security workflow is for access to PHI or in some way  identify this is not the web based registry maintenance workflow, rather more the heart of the HIE workflow and have a separate diagram for the use case to provide a gateway to a web based authentication service. Use OpenID and then it would be a pass through to use a web based UI for their registry maintenance. It would be a lighter diagram.

LT: would it be useful to document more sample use cases? DR: definitely Yes

DR: fuzzy when we say we can use this kind of end run can I just overload the functions and features of the registry and just use it for everything. Need to look at the use cases particular to the registries.

LT: speak to the team about having sample use cases that will assist with understanding the diagram

DR: Providers could also have privacy concerns and it starts to have the same privacy protection same as for patients.

Change in Time because of EDT

LT: reminder In the US the meeting will be at 10h00 (EDT) on this side it stays at 16h00 (CAT)

Meeting ended at 17h05