# Meeting/Call Notes

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

**Date:** 21-05-2013

**Attendees**

* Ryan Crichton (Jembi)
* Hannes Venter (Jembi)
* Kari Schoonbee (Jembi)
* Carl Fourie (Jembi)
* Evan Wheeler (UNICEF)
* Shahid Khokhar (Regenstrief)
* Chris Ford (ThoughtWorks)

**Meeting Notes**

Few participants due to OpenHIE strategy meeting taking place in Indianapolis

Aim is to:

1. continue review of the requirements
2. review comments on the SHR documentation
3. decide if hapy with stare byt probably not a large enough contingent to do this
4. what other tools should we be considering for review

Reviewed the document (<https://openhie.atlassian.net/wiki/pages/viewpage.action?pageId=4948134>)

1. what sort of data should be shared
2. data should be able to be retrieved in form it was sent but not neccessarily stored this way

***F09 and F010***

Keep audit logs of all interaction with clinical data

Auditing who create and when data is created - a standard requirement

Not deleting records, but keeping them

CFord – should be explicit that previous updates should still be available in the system i.e a soft delete. The principal is that system should not lose any information within the system –should all be available

RC – agree that every piece of information kept – i.e. a newer version is captured but previous version still there

CFord- Should annotate any changes to documentation

Should we audit who can view data or just updates to data

e.g. a doctor who views a patient record - should this be logged?

RC – may be useful in the future to have this type of information for reporting and to see if access has been violated

CFord –maybe two separate requirements and have different priorities

SK- we do keep a log of who is viewing data but is a separate tool – keeps track of this – not done within the SHR

CFord – maybe this should be done by the HIM?

RC – Yes, the HIM should store any interaction with data in general – SHR should store information – that feels like the right fit

CFord – agrees

RC asked SK – what is done in the Regenstrief HIE?

SK – Record updates to SHR are logged in SHR but access logged separately in application itself

***FR11- Data for secondary use***

RC- A very general requirement: how do we get information out of the system i.e. for aggregate reporting

SK – some apps require a complete of all medical records for patient – have use cases for export for a specific patent

RC- for more than 1?

SK – Do have that use case as well – to identify a cohort of patients and that data can be exported to another system

***FR12 – SHR provides extension points to allow for simple decision support***

i.e. certain hooks in SHR to allow for additional code to execute e.g. extra validation of messages or decision support functions on some messages

This seemed like an appropriate approach – to allow some to be built in but not required

If SHR deployed as standalone may not be a HIM to map terminologies and reference codes – that is thinking behind this

CFord – not sufficient to have structural validation i.e. be smart – have validation with logic

RC – Done on an interface or an extension point – can have custom service if needed but not if you don’t

SK – Does this include routing of messages e.g. for public health i.e. emergency data for surveillance purposes goes to Dept. of Health

RC – This use case could be supported – can be done in the HIM or using tis hook if SHR deployed as stand-alone

RC – Is this a suitable requirement?

CFord – Yes, think it does. Can use extension point to do a number of other things but real requirement is should be able to validate in a general purpose way – i.e. to allow semantic validation

Can’t think of another one that could be considered as a core requirement

***FR13 – Basic privacy constraints***

RC – Related to FR12 – Those hooks could be used for this

Not storing policy constraints but are able to react to them i.e. perform some logic based on policy

CFord – 1 levels – a record not accessible to a person OR some fields in that record – would describe as access control