Reviewer's report

Title: Indivo: a Personally Controlled Health Record for Health Information Exchange and Communication

Version: 1  Date: 24 July 2007

Reviewer: Pekka Ruotsalainen

Reviewer's report:

General

-----------------------------------------------------------------------------------------------

Major Compulsory Revisions (that the author must respond to before a decision on publication can be reached)= YES

This paper duplicates a lot of things already published in previous papers or can be read from web site (www.indivohealth.org). As an example, figure 1 is identical with a www-page figure. For some reason the above web address is not mentioned at all.

Instead of duplication what is already available, I am proposing that the authors will modify this paper and concentrate to the following topics:

- Description of features unique to INDIVO!
- Comparison between INDIVO and some major systems available in the market (there are more than 20, for example MyOsacar, HealthSpace, Ericson EMH and Health Hero)
- Much more clearer description of the business model of INDIVO including the financing model is needed. It is necessary to clearly describe, which kind of records are stored (e.g. original EHRs, copies or records made by the patient) by the INDIVO server. The business model should explain if the INDIVO is only a record banking system or a real service for multisource preservation and distribution of PHRs.
- The security model should be clarified. The security policy model and its implementation is not enough understandable now. Writers are speaking about two classes of security policies. Based on ISO and ASTM standards there should be a holistic security policy for the whole service including INDIVO and all connected entities. This model should be defined. As an example, it should be clarified how the data access and data disclose decisions are made (e.g. using rules, access control tables or policy based decision making model)

- Writers have missused (or misunderstood) the meaning of identity federation (token) term. This should to be corrected. If identity federation is really used, the standard/method it is based should be mentioned (e.g. identity token, SAML, attribute certificate).
- I hope also to know how the communication security and long term preservation security is achieved?

- It has been explained in this paper, that the INDIVO system is based on open standards, but no standard is mentioned. It is necessary to define which standards are used for document transfer and preservation (e.g. XML, HL7 CDA) as well as for security. I like to know if INDIVO is meeting HIPAA and/or ISO/IEC 27799 security standards?. What about audit logs, are them available?

- The writers have mentioned that the patient-doctor relationship should be secured, but it is not explained how this is realised.

The INDIVO systems has been used for 5 years. Still writers are not presenting any results or impacts. This should be one of the cornerstones of this paper.

Finally the annex including the deployment history of the INDIVO is not needed in this publication.

---

Minor Essential Revisions (such as missing labels on figures, or the wrong use of a term, which the author can be trusted to correct)

---

Discretionary Revisions (which the author can choose to ignore)

---

**What next?:** Unable to decide on acceptance or rejection until the authors have responded to the major compulsory revisions

**Level of interest:** An article of importance in its field

**Quality of written English:** Acceptable

**Statistical review:** No, the manuscript does not need to be seen by a statistician.

**Declaration of competing interests:**

I declare that I have no competing interests’ below.