Reviewer's report

**Title:** Privacy and Information Security Risks in a Technology Platform for Home-based Chronic Disease Rehabilitation and Education

**Version:** 1  **Date:** 7 December 2012

**Reviewer:** Velio Macellari

**Reviewer's report:**

Major Compulsory Revisions

The paper focuses on the risk assessment of privacy and security aspects relative to a prototype technical platform for the home environment, to be used for communication and interaction with peers and healthcare personnel.

The risk analysis presented in the paper is sound, according to the methodological basis adopted by the authors.

A point of concern, though, is that the paper does not take into account by any means the possibility that the system may be considered as a medical device, according to the Directive 93/42/EEC. Such a possibility should be carefully discussed since, if so, the risk analysis should be carried out also with a more specific instrument, namely, the standard ISO EN 14971.

Actually, ISO/IEC 27005:2011 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security. Thus, the focus is about risks that are related to information security, rather than to the patient's health status (which have been also considered throughout the paper).

The intended use of the system is not completely clear. It is stated that the technical platform for the home environment is to be used for communication and interaction with peers and healthcare personnel, and with storage of an electronic health diary containing sensor data and other information. It appears that the system manages relevant information as for the clinical status of the patient (for instance, heart rate and oxygen saturation are measured and stored, for COPD patients).

Therefore, the answer of the authors (p. 10) to the criterion “A patient should not die or have permanent reduction of health as a result of using this service” does not seem to be completely appropriate. The authors maintain that “This service is, however, not intended for use as a monitoring service and such risks will therefore not be evaluated in this risk assessment.”

It is true that the system is not a real-time monitoring service, but nevertheless a permanent reduction of health should always be considered, in principle,
whenever clinical information is not reliably shared by the stakeholders.

Another criterion for risk assessment is that “Stored information should not be permanently lost (availability breach).”

Also the statement “In our case it has no serious consequence for the patient if data registered in this system is deleted, but it would indicate that the system is not trustworthy” seems rather doubtful, since the registered data should be available to healthcare professionals when needed, for a periodic assessment of the patient’s health.

p. 15 “The worst consequence of these [availability] threats is probably that the system will lose trust and credibility and the users will stop using the service if there are too many such problems.”

The authors seem to overlook the problems associated to availability threats. Even though the system is not meant to address high-risk situations, the healthcare professionals will use it during follow-up of patients.

(Table 3) “ID= a16 - Corrupted or lost information during transfer (caused by errors), i.e. cannot be used by the intended receiver.”

Such a threat/unwanted incident is deemed by the authors as having a small consequence, i.e., the lowest degree (see Table 4). This is questionable, since the information loss could not be irrelevant as for the health status.

Moreover, corrupted information is different from lost information. In the first case, the healthcare professional may not be aware of any problem, and make a wrong decision; lost information is presumably apparent to the user of the system.

Also in the list of threats in Table 3, it is puzzling that ID “c1 - Unauthorised persons can view/read personal (sensitive) health information because the user has forgotten to switch off (or “log out” from) the RPD.” is assigned a severe consequence, whereas ID a16 (see discussion before) has a small consequence.

In conclusion, the paper could be improved by reassessing the relative importance of risks related to information security and to patients’ health status.

Minor essential revisions

p. 13 “Negligence: How easy is it to make mistakes? (Mistakes can be caused by insufficient user education or training, or by a poor user interface.)”

It is not appropriate to refer to negligence, in case of mistakes in using the system: as suggested by the authors, poor usability may also be a cause.

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