INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 80 (2011) 75–80

journal homepage: www.intl.elsevierhealth.com/journals/ijmi

The recommendations from the 2009 SiHIS working conference in Hiroshima—Issues on trustworthiness of health information and patient safety

Koji Yamamoto[a,*], *Yoshiyasu Okuhara*[b], *Eike-Henner W. Kluge*[c], *Peter R Croll*[d], *Francis Roger France*[e], *Pekka Ruotsalainen*[f], *Kiyomu Ishikawa*[g]

[a] *Suzuka University, Japan*
[b] *Kochi University, Japan*
[c] *University of Victoria, Canada*
[d] *Southern Cross University, Australia*
[e] *University Catholique de Louvain, Belgium*
[f] *National Institute for Health and Welfare, Finland*
[g] *Hiroshima University, Japan*

ARTICLE INFO

Article history:
Received 31 August 2010
Received in revised form
19 October 2010
Accepted 19 October 2010

Keywords:
Patient centered healthcare
Security
Aspect oriented
Pseudonym
Primary use
Secondary use

ABSTRACT

Held on 21st to 23rd November 2009 in Hiroshima, the SiHIS working conference aimed at finding solutions to approach to an idealistic society where (1) the individual can trust information with full understanding and responsibility, (2) the individual can allow the use of information backed by sound legitimated environment, (3) information can play its role for better healthcare and the improvement of medicine. The purpose of this paper is to propose recommendations from this working conference.

1. Introduction

In many countries, the healthcare sector is entering a time of unprecedented change due to aging populations and increasing demands for better healthcare [1]. Soaring medical expenditures have become a threat for keeping a sustainable society, challenging us to master those difficulties [1–10]. To mitigate these problems, it will be necessary to increase quality and efficiency of healthcare by fully utilizing information and communication technology (ICT) [3,10,11]. There are many eHealth implementation projects in various countries. Gordon Blackwell has estimated the near future vision of ICT use in healthcare sectors by extrapolating the developing histories of ICT [7]. According to his paper, it seems that we soon will have a seamless, fully integrated care system, in which adequate

* *Corresponding author*. Tel.: +81 59 383 8991; fax: +81 59 383 9666.
E-mail address: yama-k@suzuka-u.ac.jp (K. Yamamoto).
1386-5056/$ – see front matter © 2010 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.ijmedinf.2010.10.014

data is instantly available in the right place to ensure optimal care is provided. Indeed, there are many papers concerning interoperability of eHealth, e.g., [12,13], and HL7, which is already widely used, and may become the leading standard for interoperability of health information systems in the near future. However, as Kathrin Cresswell et al. pointed out, the history of large-scale information technology projects is littered with examples of failure [10], and this is also true for healthcare [14–18]. In any large project, acceptance of the project by the entirety of stakeholders is of crucial importance, but in the case of a large-scale information system, there are a large number and wide variety of stakeholders, so it is very difficult to have a common understanding about objectives, values, and merits [10,14]. Misunderstanding or lack of trust among the stakeholders might be a key element of difficulties occurring [19]. Eike-Henner Kluge also pointed out in his key note address the danger of believing that computer technology can solve everything [20]. It will be necessary to seek a way to improve mutual understanding and trust between all stakeholders about the content and use of information. In order to find plausible solutions to approach an idealistic society where individuals can trust information fully with complete understanding and responsibility, we organized a workshop on Security in Health Information System (SiHIS) on the *21st to the 23rd* of November (SiHIS2009) in Hiroshima. SiHIS2009 was the most recent of a long standing series of SiHIS working conferences held every three years, starting in 1976 with a first conference titled "The Achievement of Data Protection in Health Information Systems". On that very year, the International Association of Medical Informatics (IMIA) provided funds to establish its Working Group 4, and in 1979, the first working conference "Data Protection in Health Information System – Consideration and Guidelines" was held. Established as working conference, it is expected that SiHIS should pose guidelines for the use of health information. Though data protection was originally the primary target of SiHIS, the scope has become much more diversified, and at SiHIS2009 it was "The trustworthiness in health information, - issues in security and system management for patient safety". This paper reports the outcome of SiHIS2009.

2. Materials and methods

SiHIS is composed of a sequence of several workshops. At each workshop discussion points and the objectives are presented after having mini-lectures at the plenary session relating to the topic. Then several small discussion groups (SDG) were assembled as taskforces to discuss and to derive statements about topics. After two to three hours of discussions, these taskforces presented their outcomes to the plenary, and the topics were discussed again. As discussions about security are apt to be divergent, it was very important to design the discussion points and mini-lectures so that we could concentrate on the discussions. At SiHIS2009, we used two ways to call for papers: by a public call and by invitation. In the latter case, we asked a few active researchers to write a paper about the requested theme. By the middle of June 2009 we received 22 papers and selected 14 papers for the mini-lectures after scrutinizing the fitness and the quality to the theme. All 14 papers went through a strict peer review process which included at least three reviewers for each paper. By the time of the working conference, most of the papers had been revised in accordance with the reviewers' comments. The discussion points were also designed to match the mini-lectures by adding some topics derived from those papers. The number of pre-registered participants of SiHIS2009 was 57 and we could assemble three discussion groups to each workshop. The objectives and the discussion points presented to the taskforces are presented in Table 1.

Table 1 – Objectives and discussion points used at SiHIS2009.

Objective: Find solutions to reach an idealistic society where (1) the individual can trust the information with full understanding and responsibility, (2) the individual can allow the use of information backed by sound legitimated environment, (3) information can play its role for better healthcare and the improvement of medicine.
Session 1: *primary use*
Problems to solve: (1) How to improve information sharing to keep trustworthiness? (2) How to keep patient preferences in the use of information?
Discussion points (1): Improved trustworthiness: (i) How to solve the gap among the understandings of information by patients and care providers? (ii) To what extent is it necessary to resolve the gap? (iii) What is the purpose of resolving, i.e., to improve patient care or only to improve data sharing? (iv) How shall we resolve it? (v) What kind of empirical study is needed for the community to understand human behavior with respect to developing easily useable and secure electronic personal records?
Discussion points (2): Patient preferences: (i) What are the "aspects" proposed by Kung Chen [21] ? (ii) Is the use of aspects the only way to control patient preferences? (iii) Is it possible to define the concept of aspects so it is common to all societies? iv) Is it possible to combine pseudonyms and aspects?
Session 2: *Secondary Use* (Discuss about research use only)
Problems to solve: (1) Find a legal definition of de-identification: (2) Define the level of anonymity needed: (3) Find solutions to improve consensus of use.
Discussion points (1): Legal definition of de-identification: (i) Is a legal definition of de-identification possible? (ii) Is perfect de-identification a legal requisite for the research use of information without patients' consent? (iii) Are there any other cases in which data can be used? (iv) Is it necessary to enhance the legal framework for the use of research of information?
Discussion points (2): Level of anonymity needed: (i) Is perfect anonymity the key to secure the permission of society in the use of e-Health information? (ii) If no, what level of anonymity is needed?
Discussion points (3): Improve consensus of use: (i) Who should act as a gatekeeper for the patient? (ii) Can the presence of a gatekeeper controlled by the patient improve consensus of use? (iii) Are the 10 recommendations by Roger France [15] feasible in your country?
Session 3: solution
Tasks: Propose practical recommendations in the use of e-Health information and our future work; including ethical, legal and technical.
Additional discussion points: Needs for security architecture: (i) What are the implications of having a health information system with embedded security and privacy in its architecture? (ii) Can there be a standardized architecture?

3. Results

3.1. Session1: primary use

The output from the taskforces for the primary use can be divided into basic principles and recommendations:

3.1.1. Basic principles

1. Trustworthiness which goes beyond ICT, communication is important.
2. Medical records have to be understandable and accessible without compromising quality.
3. A common set of principles has been proposed, however, the fundamental merits on which those principles are based can be different. For example, America is based on liberty while the European Union is based on dignity.
4. Capacity building for clinicians, nurses and other staff, patients, other care providers e.g., family members are important.
5. Some principles are more comprehensive, e.g., observing a person's moral right, such as objection to stem cell research. This would impact on global data sharing. For example, country A is watching a person's moral right, while country B doesn't. When a de-identified dataset is transferred from A to B, it is important to check that the purpose of utilizing this dataset is not related to stem cell research. Otherwise, certain data has to be removed for someone declared that one's data should not be used for stem cell research. This can cause quite a few problems ranging from policy to detailed implementation of data sharing mechanism.
6. Aspect oriented programming [21] may be a feasible solution to support the implementation of patient preferences.

3.1.2. Recommendations for primary use

1. Patient centred healthcare is a good idea, but it needs a carefully designed implementation. How to ensure the comprehensibility of the shared information is a key question. The first sensible step is to understand the "gap" of understanding among the actors.
2. For healthcare information systems, reliability and stability is of the utmost importance. However, security and privacy policies and preferences are dynamic and evolving. How to ensure system reliability and stability while handling the ever-changing landscape of security and privacy is one of the important design issues. We think Aspect oriented programming can shed light on an incremental approach to security and privacy while keeping the main functionality of the system in tact.

3.2. Session 2: secondary use

Similarly, the following were the output for the secondary use:

3.2.1. General principles and legal framework

Secondary uses of identifiable data sets, collected primarily for other purposes, such as patient care, are mainly related to research projects, various statistics, and even administrative and commercial analyses. In principle, no identification of patient is required for secondary uses, except if tracing is necessary to assure that the same patient is not counted several times. In practice, laws on protection of private life require the designation of a "Data guardian" for each personalized data bank, responsible for external accesses and for the de-identification task, in case of secondary uses. Furthermore, the patient has to give, in writing, his authorization for use of his data, before its collection. He (she) has the right to be informed on the various secondary uses made on his data as well as on every re-identification request.

3.2.2. De-identification

Two methods are currently used to de-identify a patient:

- *anonymization*, where an individual cannot be re-identified;
- *pseudonymization*, where the individual can be re-identified.

In some cases, like in epidemiological research, where cases of dangerous communicable diseases are notifiable, in order to study incidence and prevalence, it might be needed to track back the identities of cases with similar parameters.

For these studies pseudonymization is advised. Purposes of re-identification have to be clearly stated to a Trusted Third Party (following ISO 25237) that will proceed or not to re-identification.

De-identification can never be considered as perfect. Risk assessment must be performed for defining the method to be used. More protection should be given to persons with rather unique characteristics. Unauthorized accesses have to be checked in order to improve personal health data protection. Associated demographic data might have to be removed. Some primary records might have to be kept separately to protect privacy of well known personalities.

The decision to include them or not in some research studies will depend on the patient's informed consent and on the Data guardian's decision.

3.2.3. Gatekeeper

A health professional, selected by the patient, could act as gatekeeper to help him to navigate his data as well as other sources of information. This could improve secondary uses without new legislation. However, his role should be clarified and his job might have to be paid. Will health professionals find enough time for this new function?

3.2.4. Recommendations for secondary use

In practice, security in secondary uses of health information systems has to be improved using the following measures:

1. Entrust an independent organization (a Trusted Third Party) for personal health data encryption (patient de-identification)
2. Nominate patients representatives in the management board of health data banks and health networks in order to specify with them how, by whom, and for what purposes their data can be used

3. Establish a procedure by which physicians and other health professionals can be consulted to express their voice on health matters
4. Monitor and audit all accesses to personal (even de-identified) health data, and enable each citizen to check on a user list (in data banks and in networks loggings) who had access to his health data.
5. Test systematically the security level by reviewing the accesses to patients records, the appropriateness of encryption procedures, the degree of integrity and availability of health data for secondary uses, with the help of expert systems built to detect abnormalities to be further investigated
6. Examine the secondary use protocol such as the purposes of data usage, methods of data collection, who uses the data, the role of the Data guardian.
7. Detect linkage to other data bases and audit legally accessed records by court orders or by authorized security agencies
8. Check systematically every request for re-identification of a citizen in de-identified data bases, mainly in case of genetic registers or psychiatric records
9. Detect fraud in identity of requesters of access to health data bases
10. Apply and diffuse sanctions for unauthorized accesses, fraud in identification and damage caused to a patient by leakage of confidential information.

3.3. *Session 3: solutions*

As stated in the introduction, the problem is not so simple to reach consensus about solutions and future work even among the specialists. Indeed, the three taskforces have reached different conclusions which are partly contradictory each other. We will discuss this part a bit more in the next chapter.

4. Discussions

4.1. *Flavour of session 3*

One of the taskforces started discussions about the needs for security architecture. The outcome of the discussion was that it is inevitable to use an architectural framework like the GCM that formally describes structure and functions of a system specialized for the different domains (aspects) reflected by that system and using domain-specific concept representations, but also covering the system's development process [22]. The domains range from medicine through technology, administration up to ethics. This taskforce thought that legal and ethical aspects could be integrated in an architectural framework. As for the future work of SiHIS, this taskforce pointed out the need for dealing with the challenge of globalization, and for awareness and training on security, privacy, safety and ethics for health professionals.

The second taskforce concluded that security policy models cannot solve all problems. Ethics should be included. There is no need to propose any specific security architecture. There are many solutions available, and privacy issue is a key point in the case of sharing information. This group also pointed out the importance of thinking about the balance between patient's rights and quality of care, e.g., positive and negative impacts should be analyzed in such situations that a patient has access to his own EHR. As for the future work, this taskforce pointed out the need for looking at what is going on outside our health care domain, e.g., security and privacy development of the Semantic Web, and focusing on common global problems.

The last taskforce started discussions about legal framework, since usability issues with individuals accessing their own records will soon be solved technically. The members of this taskforce reached the consensus that we do not have sufficiently well defined legal framework internationally, but implementation of technical applications will spread in some areas irrespective of legal framework. Therefore it will be necessary to establish an evaluation standard for implementations that every technical product should meet. This taskforce pointed out the importance of a working group which undertakes a case study to develop and improve the process for evaluation.

Each taskforce was asked to propose practical recommendations in the use of e-Health information. But as this objective was vague and the multi-faceted output of each taskforce may not have focused on this objective. As shown above, even among the specialists there are a wide variety of ideas and it will be necessary to communicate with each other in order to bridge the gap. Though creation of secure ICT infrastructure would be a prerequisite to improve the use of ICT, in order to improve trustworthiness it will be necessary to create a society where we can understand and trust each other. As Vimla Patel et al. stated while proposing a cognitive framework to share the very essence of patient health records with adolescent depressed patients [23], it will be necessary to explore the ways to improve the comprehensibility of pertinent users.

4.2. *The selected papers in this edition*

As stated, 14 papers were adopted in SiHIS2009 plus the one key note. Most of them were peer reviewed at least three times, some of them were revised in accordance with reviewer's comments, and all of them have good qualities as scientific papers. Just after the SiHIS2009, K. Yamamoto, the chair of SPC, also asked all the authors to improve their papers to avoid overlapping of publication. However, due to a limitation of pages not all papers were selected. For the selection process, the chair of SPC requested voting by all the SPC members, OC members and the chairs of each session. He asked all these core members to select at most 5 papers which they thought would contribute most to the present conference and add scores of "must" or "better" to include in this special edition. Fourteen members attended to this voting program and, fascinatingly, most of them selected the same papers.

The cornerstone of E.W. Kluge's key note was about the danger of over-reliance on computer technology [20]. Roger France described the need of gatekeepers for the secondary use of information [15]. Sebastian Haas et al proposed a privacy-protecting approach to information systems for controlled disclosure of personal data to third parties [24]. Peter Croll discussed a framework for determining privacy policy [25], which will help system designers make person-centered

Summary points

- 1. Summarize the outcomes of the IMIA security working conference, SiHIS, in the form of recommendations of the use of health information.
- 2. Practical and feasible solutions towards the creation of patient centered trustworthy environment are suggested.

health systems, while Bernd Blobel offered an architectural framework for designing ontology-driven systems intelligently ruling privilege management and access control [22]. The use of pseudonym proposed by Catherine Quantin et al will be another practical way of information sharing at care settings [26]. Since health information stored at other institutions will only be necessary at the time of care, i.e., where patients are present, there are plenty of possibilities to include patients' preference into pseudonym. All of the papers included in this special edition will pave the way towards the creation of patient centered trustworthy environment.

Acknowledgement

SiHIS2009 was chaired by Kiyomu Ishikawa and François-André Allaert, and it is the support of many participants working as the member of SPC, OC, and the chairs of small discussion group (SDG) that SiHIS2009 became a great success. We express sincere thanks to all of them. Following, those members are listed to express our sincere thanks.

SPC Members: Albert Reinder Bakker, Jochen Moehr, Eike-Henner W. Kluge, Francois A. Allaert, Francis Roger France, Peter Croll, Bernd Blobel, Vimla Patel, Pekka Ruotsatainen, Catherine Quantine, Da Wei Wang, Koji Yamamoto

OC Members: Yoshiyasu Okuhara, Andrew Georgiou, Yukio Kurihara, Tomiaki Morikawa, Haruhiko Nishimura, Norio Sasagawa, Hajime Nakagawa, Takaya Sakusabe

SDG Chairs: Hiroshi Inada, Da-Wei Wang, Andrew Georgiou, Francis Roger France, Vimla Patel, Yoshikazu Nakamura, Bernd Blobel, Peter Croll, Pekka Ruotsalainen.

REFERENCES

[1] R. Haux, J. Howe, M. Marschollek, M. Plischke, K.H. Wolf, Health-enabling technologies for pervasive health care: on services and ICT architecture paradigms, Inf. Health Soc. Care 33 (2) (2008) 77–89.
[2] R. Haux, Individualization, globalization and health—about sustainable information technologies and the aim of medical informatics, Int. J. Med. Inform. 75 (2006) 795–808.
[3] B. Chaudhry, J. Wang, S. Wu, et al., Systematic review: impact of health information technology on quality, efficiency, and costs of medical care, Ann, Intern. Med. 144 (10) (2006) 742–752.
[4] Francis J. Crosson, 21st-Century health care—the case for integrated delivery systems, N. Engl. J. Med. 361 (October (14)) (2009) 1324–1325.
[5] T. Bodenheimer, R. Berry-Millett, Follow the money—controlling expeditures by improving care for patients needing costly services, N. Engl. J. Med. 361 (October (16)) (2009) 1521–1523.
[6] M. Tsiknakis, A. Kouroubali, Organizational factors affecting successful adoption of innovative eHealth services: a case study employing the FITT framework, Int. J. Med. Inform. 78 (2009) 39–52.
[7] Gordon Blackwell, The future of IT in healthcare, Inf. Health Soc. Care 33 (4) (2008) 211–326.
[8] Chung-Chih Lin, Ren-Guet Lee, Chun-Chieh Hsiao, A pervasive health monitoring service system based on ubiquitous network technology, Int. J. Med. Inform. 77 (2008) 461–469.
[9] Steven Shea, George Hripcsak, accelerating the use of electronic health records in physician practices, N. Engl. J. Med. 362 (January (3)) (2010) 192–195.
[10] K. Cresswell, A. Sheikh, The NHS Care Record Service (NHS CRS): recommendations from the literature on successful implementation and adoption, Inf. Primary Care 17 (2009) 153–160.
[11] D.A. Ludwick, John Doucette, Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries, Int. J. Med. Inform. 78 (2009) 22–31.
[12] Implementing Secure Healthcare Telematicse Applications in Europe, edited by the ISHTAR Consortium, IOS Press, 2001.
[13] eHealth: Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge, edited by Bernd Blobel, Peter Pharow, Michael Nwelich, IOS Press, 2008.
[14] Ian Herbert, Simon de Lusignan, Further changes are needed if the national care record service (NCRS) implementation is to succeed, Commentary, Inf. Primary Care 17 (3) (2009) 161–164.
[15] Francis Roger France, E-health in Belgium, a new "Secure" federal network: role of patients, health professions and social security services, Int. J. Med. Inform., this special edition.
[16] A.K. Jha, D. Doolan, D. Grandt, T. Scott, D.W. Bates, The use of health information technology in seven nations, Int. J. Med. Inform. 77 (2008) 848–854.
[17] H. Pirnejad, R. Bal, M. Berg, Building an inter-organizational communication network and challenges for preserving interoperability, Int. J. Med. Inform. 77 (2007) 818–827.
[18] A. Hoerbst, C.D. Kohl, P. Knaup, E. Ammenwerth, Attitudes and behaviors related to the introduction of electronic health records among Austrian and German citizens, Int. J. Med. Inform 79 (2010) 81–89.
[19] P. Garside, Organizational context for quality: lessons from the fields of organizational development and change management, Quality in Health Care 7 (1998) S8–S15 (Suppl).
[20] E. W. Kluge, Ethical, Legal challenges for health telematics in a global world: telehealth and the technological imperative, Int. J. Med. Inform., this special edition.
[21] K. Chen, D.W. Wang, Supporting patients' privacy preferences using aspects, Jpn. J. Med. Inform. 29 (2010) 117–128.
[22] B. Blobel, Ontology Driven Health Information Systems Architectures Enable pHealth for Empowered Patients, Int. J. Med. Inform., this special edition.
[23] V.L. Patel, S. Myneni, Facilitating patients' safe access to electronic health records: a proposed cognitive framework, Jpn. J. Med. Inform. 29 (2010) 109–116.
[24] S.Haas, et al, Aspects of privacy for electronic health records, Int. J. Med. Inform., this special edition.

[25] P.R. Croll, Determining the Privacy Policy Deficiencies of Health ICT Applications through Semi-Formal Modelling, Int. J. Med. Inform., this special edition.

[26] C. Quantin, et al., Medical record search engines, using pseudonymised patient identity: an alternative to centralized medical records, in this special edition of Int. J. Med. Inform.