Impact of ICT on Home Healthcare

Sokratis Vavilis, Milan Petković, Nicola Zannone

Impact of ICT on Home Healthcare

Sokratis Vavilis[1], Milan Petković[1,2] and Nicola Zannone[1]

[1] Eindhoven University of Technology, Netherlands
{s.vavilis, n.zannone}@tue.nl
[2] Philips Research Eindhoven, Netherlands
milan.petkovic@philips.com

Abstract. Innovation in information and communication technology has a great potential to create large impact on modern healthcare. However, for the new technologies to be adopted, the innovations have to be meaningful and timely, taking into account user needs and addressing societal and ethical concerns. This paper focuses on ICT innovations related to the home healthcare domain. To ensure the adoption of new healthcare services, the new innovative technologies need to be complemented with new methods that can help patients to establish trust in healthcare service providers in terms of privacy, reliability, integrity of the data chain and techniques that help service providers to assess the reliability of information and data contributed by patients. This paper sketches various lines of research for the development of trusted healthcare services namely, patient compliance, reliability of information in healthcare, and user-friendly access control.

Keywords: healthcare security, home healthcare, trust management

1 Introduction

The high bandwidth connectivity provided by the Internet enables new services to support citizens in their daily lives. An important category of these services is healthcare services. The first examples of these services already exist today, and soon new services will emerge offering increased sophistication and improved but cheaper healthcare. An exponential growth of these services is expected, due to two tendencies. First, demand for care and cures will increase over the next decades caused by the ageing population (within 40 years, one in every four people will be over 60). Secondly, the number of healthcare workers is expected to diminish relative to the total population (without changes to the healthcare system, 25% of the working population would be needed to provide today's level of care by 2040 in a typical western country). New ICT supported healthcare services can overcome this problem by allowing people not to rely only on traditional care. However, to ensure the adoption of new healthcare services, the new innovative technologies need to be complemented with new methods that can address related ethical and societal issues.

adfa, p. 1, 2011.

A good example is home healthcare. Current home healthcare services are rudimentary in nature. Often they rely on call centers or nurses visiting the patient while new propositions are based on the Internet. One of the important impediments for the use of the Internet is the lack of trust. Trust is a requirement for the widespread adoption of healthcare services by clients (patients), by caregivers and by the parties that are financially responsible.

Existing techniques address part of the trust and security requirements, for example tools for identity management and for encryption of connections. Missing are techniques that help end-users to establish trust in a healthcare service in terms of privacy, reliability, integrity of the data chain, as well as techniques that help physicians to assess the reliability of information and data contributed by patients. There is a need for an integrated and easy to understand approach to trust in terms of security, privacy, and transparency, where users can make informed decisions whether to trust a service and can control the usage of their personal information.

In this paper, we present the research lines for trust management in home healthcare services. Home healthcare services aim to support people who are chronically ill or who are rehabilitating. These services gather patient's sensitive information that is then interpreted by medical professionals to manage their diseases. The adoption of such services, however, hardly relies on the patients' trust in a healthcare service provider in terms of privacy of the data chain and physicians' trust in the reliability of information and data contributed by patients. In particular, a number of questions should be addressed:

- How can compliance with a treatment be reliably measured?
- Can a physician trust data measured by a patient at home?
- How can patients use home healthcare services while ensuring their privacy and controlling the use of information in a simple intuitive way?

Answers to these questions require investigating different research lines including patient compliance, reliability of information in healthcare, and user-friendly access control. The paper discusses the existing proposals in these areas and describes a research plan for enhancing the state-of the-art.

The structure of the paper is as follows. The next section presents the impact of ICT innovation on healthcare. Section 3 discusses the problem of trust towards healthcare services. Section 4 discusses trust management for home healthcare services. Finally, Section 5 concludes the paper providing directions for future work.

2 ICT innovation in Healthcare

The advance of ICT technologies is leading to the design of novel electronic healthcare services that improve people's health and well-being but also extend beyond the individual towards sustainability of our society. Consequently, many countries created policies to foster innovation and spread the successful adoption of these technologies in their healthcare sector. In this process of innovation creation it is crucial to focus on meaningful innovations, sustainability, and societal and ethical values

underpinning the innovations. Meaningful innovation means new ideas, new approaches, new solutions that make lives healthier, more enjoyable, and more productive. It also means that they should be driven by user needs (not by technology), taking into consideration economic, societal and environmental sustainability. They should be well timed and introduced when they really make sense.

In healthcare, we witness many examples of such innovations ranging from electronic health records (EHRs), clinical decision support systems, via medical apps for mobile devices to next generation gene sequencing. The creation of national/regional EHR infrastructures such as RHIO's in the US, the NHS Spine project in the United Kingdom and NICTIZ in the Netherlands, is complemented with efforts on creating commercial Web-based personal health record (PHR) systems such as Microsoft HealthVault. These applications process, store, and exchange patient's medical information and allow for harnessing big data to improve healthcare.

Clinical decision systems assist healthcare providers with decision making tasks. They allow clinicians to take into account all important clinical observations and up-to-date clinical knowledge when diagnosing and treating patients.

Advances in mobile Health (mHealth) allow healthcare providers and patients to take part in a revolution in the way healthcare information is accessed and delivered. Healthcare providers and patients can access the most up to date medical resources anytime anywhere on their mobile devices.

New technologies for genome sequencing will make possible that everyone's genome is sequenced quickly for an affordable price, which is expected to decrease to one thousand dollars very soon. This will allow not only quick and cheap sequencing, but it will allow for the use of genomics in diagnostics and treatment enabling personalized medicine.

Finally, there are an increasing number of extramural telemedicine applications in the home healthcare domain such as remote patient monitoring (RPM). RPM systems combine consumer electronics and the Internet to connect patients and their care providers, thus enabling new care models. They allow patients to stay at home attached to monitoring devices/sensors that are getting smaller and wireless. In this way, patient's physiological and other contextual data can be collected and transmitted to remote care providers for review or intervention. Typically, RPM systems comprise several measurement devices (such as a blood pressure meter, weighing scale or glucose meter) a medical hub device that collects the data from measurement devices and sends them to a backend service. Furthermore, a hospital EHR or PHR systems are also considered as part of this eco system (the measurement data are sent from the medical hub to a PHR system, but in certain cases they are sent from the medical hub to a backend service which forwards them to an EHR or PHR system). A typical architecture of an RPM system as defined by the biggest standardization initiative in the domain of personal healthcare, called Continua Health Alliance[1] is shown in figure 1.

In this paper we will focus on home healthcare technologies, as they are very controversial. On one hand, these technologies improve the quality of patient life (he can stay at home), and provide faster and cheaper healthcare services. On the other hand,

[1] http://www.continuaalliance.org

they are exposed to different security and safety threats as the patient is far from healthcare providers, and it becomes simpler to collect, store, and search electronic health data, thereby endangering people's privacy.

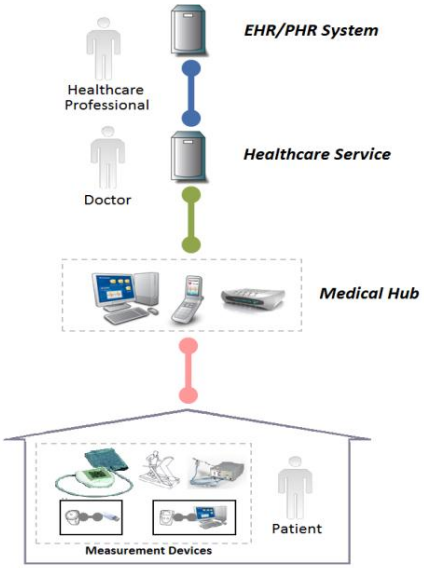

Fig. 1. Architecture of an RPM system.

3 Trusted Healthcare Services

Electronic healthcare services offer important economic and social benefits for our society. Patients rely on these services for their safety and care and for improving their quality of life. For physicians, electronic health and wellness services offer support for providing more effective and continuous care. For insurers and governments, these services bring a reduction of costs, and for commercial service providers, this is a new business opportunity. However, electronic healthcare services cannot be exploited until the trust question has been addressed in a fundamentally correct way.

Indeed, trust is a pre-requisite for the acceptance of these services by end users. Trust establishment is crucial for physicians and service providers as they will use healthcare services to implement and extent (medical) treatments. In particular, healthcare providers need to trust the patient data they obtain remotely from the measurement devices deployed in patient's home. It is crucial for them to know that a vital sign of a registered user is measured (not of his friends/children), that the measurement was taken with a certified device, under standardized conditions (e.g., with the blood pressure cuff on the arm at the heart level) and that it is not obtained as a result of device malfunctioning.

In a healthcare setting, trust is also of special relevance because healthcare services deal with very personal and private information. Home healthcare services monitor patients and gather data that are interpreted by medical professionals. Health and wellness services support people in need in many ways on the basis of personal and health related information. People in health communities share health and well-being information which then becomes potentially available to the whole community and beyond.

Privacy is a major concern of many citizens and the government has an important role in protecting the privacy of the citizen [1]. Therefore, the government has developed legislation to protect its citizens, who may make use of the legal facilities provided. For example, on December 17, 2008, 2% of the Dutch population (330.000 people) had submitted objection forms to the Dutch Ministry of Health, stating that their electronic health records cannot be shared electronically.[2]

To facilitate the acceptance of electronic healthcare services, it is necessary to develop the technology that help end users to establish trust in healthcare service providers in terms of privacy, reliability, integrity of the data. Standard Internet security techniques provide authentication and encryption of the communication with a service provider. However, they do not provide the user with means to control or even know how a service provider will actually use their personal information. It is important to have mechanisms in place that allow users to make an informed decision to trust a service provider on the basis of facts, such as reputation and security attributes.

The THeCS project addresses the very important trust questions (transparency, privacy and security) for healthcare services. THeCS is a Dutch national project in the COMMIT program with 11 partners including representatives from industry, Dutch research institutes, Dutch universities and hospitals. The project addresses trust as one of the key issues for new electronic healthcare services. It will create measurable and enforceable trust. This notion is new for electronic healthcare services (and for Internet services in general), and it is fundamental for their success. The objective of THeCS is to create new techniques for measuring and controlling the reliability and use of (healthcare) information. These techniques allow users and service providers to trust each other and to benefit from these new services.

The concrete goal of the THeCS project is to create and define:

- Ethical, legal, sociological and psychological requirements for trust in healthcare services. The spectrum of healthcare services is very wide, ranging from formal medical services to pure commercial services that support every day activities. Often these services share information. It is this integration of services from different domains and information sharing that is of particular interest.
- A technical protocol to reliably assess the quality of medical data (e.g., blood pressure) measured by patients at home, including the identification of the patient, compliance with the specified measurement protocol, and certification of the measurement device.

[2] See www.minvws.nl/kamerstukken/meva/2008/bezwaarprocedure-epd.asp.

- A cryptographic technology that enables health service providers to process encrypted medical information so that only intended operations are possible and that information is not disclosed otherwise. A specific example is categorization of a community into groups of patients with similar (according to a definition relevant for healthcare) characteristics, without disclosing the characteristics of individual patients.
- A cryptographic technology for privacy preserving data mining of patient health data to support clinical research and knowledge creation for clinical decision support systems.

In the remainder of this paper, we will focus on trust management for home healthcare services.

4 Trust Management for Home Healthcare Services

Home healthcare services have been proposed to decrease the cost of healthcare while making it more comfortable for the patient. These services aim to support people who are chronically ill (e.g., post-stroke, diabetes, Chronic Obstructive Pulmonary Disease (COPD)) or people who are being rehabilitated. They monitor the health and well-being of people, enabling tailored assistance where and when needed. In particular, they gather sensitive personal information that is then interpreted by medical professionals in order to provide treatment. The adoption of such services, however, hardly relies on the trust that both patients and medical professionals have in the provided healthcare services. In particular, a number of questions should be addressed:

- How can compliance with a treatment be reliably measured? Patients' adherence to medication and to the treatment in general (e.g., activities, exercises, dietary guidelines) is a fundamental factor for the success of a treatment. However, treating a certain disease usually requires a variety of different medication schemes and treatment plans, making the compliance checking a complex task.
- Can a physician trust data measured by a patient at home? Home healthcare patients measure physiological parameters at home and a physician uses the data to make treatment and diagnosis decisions. It is very important that the measurements are accurate and that a physician can accept them as medical information.
- Patients and consumers want the possibility to control their personal health information. How can patients use home healthcare services while ensuring their privacy and controlling the use of information in a simple intuitive way?

Answering these questions requires developing the technology for physicians and other users of measured home healthcare information to easily determine the trustworthiness of the information and patient compliance. Moreover, there is the need of user-friendly technologies which will allow patients to control the processing and sharing of their information. In the remainder of the section, we discuss various research lines to address these challenges.

4.1 Patient Compliance

In home healthcare services, patients do not receive treatment (e.g., medication, rehabilitation) directly at the hospital; rather, healthcare service providers prescribe treatment to their patients who should follow such a treatment at home. This, however, leads to a question on how to assess patient compliance with the prescribed treatment.

Compliance with a medication regimen or a treatment is generally defined as the extent to which patients take medications and follow the treatment as indicated by their healthcare providers [2]. The adherence to a treatment by the patient is crucial both for the treatment evaluation and for the patients' recovery. However, given the large range of existing treatments, patient compliance is difficult to assess.

Several solutions for patient compliance have been proposed in the literature. A number of proposals focus on medication adherence. Here, compliance measurement methods can be classified in direct and indirect methods [2]. Direct methods measure, for instance, concentration of a drug or its metabolite in some biologic factor such as blood. Indirect, methods are based on the assessment of clinical responses by medical professionals, patient questionnaires about adherence, patient diaries, and pill counting. Other types of adherence measurements [3-6] include medication possession ratio and related measures of medication availability, discontinuation/continuation, switching, medication gaps, refill compliance, and retentiveness/turbulence. A comprehensive list of existing methods is presented in [7].

An example of an indirect method is proposed in [8]. This work aims to identify hypertensive patients who do not adhere to prescribed medication using an ontology based approach. In particular, patient information such as patient prescription details, medication possession ratios and blood pressure measurements are specified in an ontology. Adherence of patients to medication is then determined by querying the ontology using non-adherence criteria (e.g., patient who have lapsed in taking their medication while having a low medication possession ratio).

Recently, advances in patient monitoring systems have made possible to remotely monitor the patient to keep track of his health status, as well as providing limited abilities to monitor compliance. Such solutions include, for instance, the application of body sensors [9-11], smart device integration for patient monitoring [12, 13] and event-based methods [14], which aim to capture the patient's activities and vital metrics. In addition, some preliminary work on patient compliance prediction has been done by applying statistical methods and text mining techniques [15].

In summary, several efforts have been devoted to the definition of methods for treatment adherence. However, existing solutions only concentrate on a specific type of treatment such as medication adherence or monitoring of patients' activities. These efforts are insufficient in practice as the treatment for certain diseases often consists of different types of treatments. The effectiveness of the treatment can be assessed only by assessing and combining the adherence to the single treatments.

Providing a solution for patient compliance to the treatment still remains a challenge. In particular, we need comprehensive solutions for measuring patient compliance for home healthcare services. The development of such solutions requires investigating and integrating existing measurement mechanisms for patient compliance.

The study should not be limited to existing solutions specific for healthcare, but it should consider compliance checking techniques proposed in other domains like privacy and business process [16,17].

4.2 Reliability of Information in Healthcare

To assess patient health status, healthcare providers have to rely on measurements which may have been taken directly by the patients. Thus, trust and reliability of the measurements is a necessary condition for the acceptance of the service by healthcare providers. Next to ensuring proper patient/device authentication, data authenticity and integrity, it is important to capture the correctness of the authentication process too. An overall solution that can capture all these aspects is the application of reputation systems, where providers build a level of trust in the patient based on his ability to take measurements [18].

Reputation systems have been studied in the literature for different domains, such as auction websites and peer-to-peer sharing networks [19]. Lately, reputation systems have been proposed for healthcare. Most existing approaches, however, focus on the patient perspective, where patients rate the services of doctors and healthcare providers via a web portal or a health oriented network [20, 21]. Conversely, very few studies address patients' trustworthiness from the perspective of healthcare providers and in particular the reliability of measurements taken by patients. Existing proposals [18, 22] mainly focus on the reliability of the data maintained in the form of electronic and personal health records.

Additional problems appeared with the use of web portals rating healthcare services. Patients often subscribe to expert websites and search information regarding their illness on the Internet. Although this practice may have advantages, the major drawback concerns the trustworthiness of information. For instance, in Revolution Health[3] and other similar online community reputation systems, the trustworthiness of information is assessed only by considering the information source. To assure information trustworthiness we also need to consider the information itself [23, 24].

Summarizing, there are no comprehensive studies on assessing the trustworthiness of patients' measurement and on addressing the problem of trust in home healthcare services. Moreover, to reassure patient safety, a method for measuring the trustworthiness of information originating from the Internet should be integrated. An interesting research challenge is, thus, the design of solutions for measuring information trustworthiness for home healthcare that also address the trust issues related to Internet data. We believe that a reputation-based solution can ensure the reliability of home healthcare data needed by physicians. To this end, it is necessary to investigate the issue of data trustworthiness from both healthcare providers and patients' perspectives and elicit the requirements for reputation systems to be deployed in healthcare systems. To get such systems accept by end-users, information on data reliability should be easily accessible and understandable. Therefore, methods for assessing data

[3] http://www.revolutionhealth.com/

reliability should be coupled with methods and tools that visualize indicators for data reliability in a way that is understandable by end-users.

4.3 User Friendly Advanced Access Control

Healthcare services deal with very personal and sensitive information. The protection of sensitive information is usually enforced using access control. Several access control models have been proposed in the literature (see [25] for a survey). In particular, access control for the healthcare domain has been intensively studied in [26-28]. The challenge in designing an access control system for healthcare is that, while posing strict constraints on the access to sensitive information, the system has to cope with the dynamic environment of healthcare and the potential exceptions that are raised in emergency cases. Furthermore, medical data can also be formed as arbitrary text, such as a patient report made by healthcare practitioners, leading to the need for policies based on content. In this trend, content-based access control [29, 30] and tag-based access control [31] methods have been proposed. For instance, content-based approaches have been used for the protection of medical images [32]. Although these access control models are very expressive and allow the specification of a wide range of authorization policies, they are usually difficult to use by end users.

The last years have seen an increasing interest in the development of user friendly privacy management and access control systems. For instance, various enterprises designed platforms which allow users to set their privacy and access control policies. One example is Google dashboard privacy tool, which through a web interface displays to users what information about them is stored and who can access it. Similarly, social networks such as Facebook let users restrict or grant access to other users or groups on their data (e.g., wall posts, photos). Although these proposals provide a simple and straightforward solution, they neither allow users to understand the effect of the specified policies nor ensure secure access control.

Therefore, a need for more flexible yet friendly privacy management exists. Efforts such as privacy dashboard[4], PrivacyOS project[5], Primelife project[6]) and privacy room [33] provide tools (e.g., browser add-ons, mobile applications) for regulating the exposure of user data to the network. Pearson et al. [34] propose a client privacy management scheme based on data obfuscation (not necessarily using encryption) and user "personas." Although these proposals increase usability and flexibility, they do not provide users with the overview of the effect of the specified policy.

In conclusion, although several studies on access control have been carried out, no comprehensive studies on user-friendly access control for healthcare exist. The challenge is to define a novel access control model that guarantees an appropriate level of security and allows users to specify the policies regulating the exposure of their information to others. In addition, the model should be easy to use by end users. Ideally, the access control system should not only allow users to define access rules to their

[4] http://code.w3.org/privacy-dashboard/wiki
[5] https://www.privacyos.eu/
[6] http://www.primelife.eu

data but also to support them in "visualizing" the effect of the defined access control policy and therefore in ensuring that the created policy reflects users' intentions. The lack of such an overview might result in a loss of sensitive information. As an example, a patient affected by HIV might want to prevent the disclosure of information regarding his medical condition, restricting access to information regarding his disease (e.g., HIV status, HIV antibodies). However, the patient might not restrict access to other fields (e.g., white blood cell count, CD4 T-cells count) from which, although they do not contain his HIV status, his disease may be inferred.

The design of a user-friendly access control model requires that we divide the access control model conceptually into two layers: a high-level layer, in which end users can specify privacy preferences, and a low-level layer, which consists of machine-readable policies eventually enforced by the system. The refinement and mapping of high-level policies (specified by users) into enforceable policies can be achieved, for instance, by enabling semantic interoperability between high-level descriptions of information to be protected and the data objects in which such information is stored. The aim of this semantic alignment is to support the automatic generation of enforceable policies from the high-level policies specified by users. As a result, enforceable policies can be dynamically customizable with respect to user preferences.

5 Conclusions

The growth of the Internet and ICT technologies had a large impact on modern healthcare. A fundamental need is to design novel electronic healthcare services that improve people's health and well-being but also extend beyond the individual towards sustainability of our society. However, although the use of ICT in healthcare can offer several benefits to society, the adoption of electronic healthcare services relies also on ethical and societal aspects such as the trust that end users (e.g., patients and physicians) have towards such services. This paper discussed the challenges for developing trusted home healthcare services. The THeCS project addresses the issue of trust in healthcare services. In particular, the project aims to define the technology necessary to deploy trusted healthcare services. We presented various lines of research that will be also investigated within the project to address such challenges, namely patient compliance, reliability of information in healthcare, and user-friendly access control.

Acknowledgements

This work has been done in the context of the THeCS project which is supported by the Dutch national program COMMIT.

References

1. Guarda, P., Zannone, N.: Towards the development of privacy-aware systems. Inf. Softw. Technol. 51(2), 337–350 (2009)

2. Osterberg, L., Blaschke, T.: Adherence to medication. New England Journal of Medicine 353(5), 487–497 (2005)
3. Hess, L., Raebel, M., Conner, D., Malone, D.: Measurement of adherence in pharmacy administrative databases: a proposal for standard definitions and preferred measures. The Annals of Pharmacotherapy 40(7/8), 1280–1288 (2006)
4. Steiner, J., Prochazka, A.: The assessment of refill compliance using pharmacy records: methods, validity, and applications. Journal of Clinical Epidemiology 50(1), 105–116 (1997)
5. Halpern, M., Khan, Z., Schmier, J., Burnier, M., Caro, J., Cramer, J., Daley, W., Gurwitz, J., Hollenberg, N.: Recommendations for evaluating compliance and persistence with hypertension therapy using retrospective data. Hypertension 47(6), 1039–1048 (2006)
6. Leslie, S., Gwadry-Sridhar, F., Thiebaud, P., Patel, B.: Calculating medication compliance, adherence and persistence in administrative pharmacy claims databases. Pharmaceutical Programming 1(1), 13–19 (2008)
7. Andrade, S., Kahler, K., Frech, F., Chan, K.: Methods for evaluation of medication adherence and persistence using automated databases. Pharmacoepidemiology and Drug Safety 15(8), 565–574 (2006)
8. Mabotuwana, T., Warren, J.: A Semantic Web Technology Based Approach to Identify Hypertensive Patients for Follow-Up/Recall. In: Proceedings of the 21st IEEE International Symposium on Computer-Based Medical Systems, pp. 318–323. IEEE Press, New York (2008)
9. Reiter, H., Maglaveras, N.: HeartCycle: Compliance and effectiveness in HF and CAD closed-loop management. In: Proceedings of Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 299–302. IEEE Press, New York (2009)
10. Otto, C., Milenković, A., Sanders, C., Jovanov, E.: System architecture of a wireless body area sensor network for ubiquitous health monitoring. J. Mob. Multimed. 1(4), 307–326 (2005)
11. Alemdar, H., Ersoy, C.: Wireless sensor networks for healthcare: A survey. Comput. Netw. 54(15), 2688–2710 (2010)
12. Schmidt, S., Sheikzadeh, S., Beil, B., Patten, M., Stettin, J.: Acceptance of telemonitoring to enhance medication compliance in patients with chronic heart failure. Telemedicine and e-Health 14(5), 426–433 (2008)
13. Pang, Z., Chen, Q., Zheng, L.: A pervasive and preventive healthcare solution for medication noncompliance and daily monitoring. In: Proceedings of the 2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies, pp. 1-6. IEEE Press, New York (2009)
14. Mouttham, A., Peyton, L., Eze, B., Saddik, A.: Event-driven data integration for personal health monitoring. Journal of Emerging Technologies in Web Intelligence 1(2), 110–118 (2009)
15. Petrou, C.: Use of text mining to predict patient compliance. SAS Global Forum, ProQuest (2008)
16. Banescu, S., Zannone, N.: Measuring privacy compliance with process specifications. In: Proceedings of the 7th International Workshop on Security Measurements and Metrics, pp. 41-50. IEEE Press, New York (2011)
17. Petković, M., Prandi, D., Zannone, N.: Purpose Control: did you process the data for the intended purpose? In: Proceedings of the 8th VLDB Workshop on Secure Data Management. LNCS 6933, pp. 145–168. Springer-Verlag, Berlin, Heidelberg (2011)
18. van Deursen, T., Koster, P., Petković, M.: Hedaquin: A Reputation-based Health Data Quality Indicator. Electron. Notes Theor. Comput. Sci. 197(2), 159-167 (2008)

19. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support Syst. 43(2), 618–644 (2007)
20. Jøsang, A.: Online reputation systems for the health sector. Electronic Journal of Health Informatics 3(1), e8 (2008)
21. Ebner, W., Leimeister, J.M., Krcmar, H.: Trust in Virtual Healthcare Communities: Design and Implementation of Trust-Enabling Functionalities. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences, pp. 70182a. IEEE Press, New York (2004)
22. Alhaqbani, B., Jøsang, A., Fidge, C.: A medical data reliability assessment model. J. Theor. Appl. Electron. Commer. Res. 4(2), 64–78 (2009)
23. Bertino, E., Dai, C., Kantarcioglu, M.: The challenge of assuring data trustworthiness. In: Proceedings of the 14th International Conference on Database Systems for Advanced Applications. LNCS 5463, pp. 22-33. Springer-Verlag, Berlin, Heidelberg (2009)
24. Moturu, S.T., Liu, H., Johnson, W.G.: Trust evaluation in health information on the World Wide Web. In: Proceedings of the 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 1525–1528. IEEE Press, New York (2008)
25. Samarati, P., De Capitani di Vimercati, S.: Access control: Policies, models, and mechanisms. In: Foundations of Security Analysis and Design. LNCS 2171, pp. 137–196. Springer-Verlag, London, UK (2000)
26. Zhang, L., Ahn, G.J., Chu, B.T.: A role-based delegation framework for healthcare information systems. In: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies, pp. 125-134. ACM, New York (2002)
27. Becker, M.Y., Sewell, P.: Cassandra: Flexible Trust Management Applied to Electronic Health Records. In: Proceedings of the 17th IEEE Workshop on Computer Security Foundations, pp. 139–154. IEEE Press, New York (2004)
28. Røstad, L.: Access control in healthcare information systems. PhD thesis, Norwegian University of Science and Technology (2008)
29. Hart, M., Johnson, R., Stent, A.: More Content - Less Control: Access Control in the Web 2.0. In: In: Proceedings of Web 2.0 Security and Privacy Workshop (W2SP'07) (2007)
30. Giuri, L., Iglio, P.: Role templates for content-based access control. In: Proceedings of the 2nd ACM Workshop on Role-Based Access Control, pp. 153–159. ACM, New York (1997)
31. Hinrichs, T.L., Garrison, W.C., Lee, A.J., Saunders, S., Mitchell, J.C.: TBA: A Hybrid of Logic and Extensional Access Control Systems. In: Proceedings of the 8th International Workshop on Formal Aspects of Security and Trust (2011)
32. Tzelepi, S.K., Koukopoulos, D.K., Pangalos, G.: A flexible content and context-based access control model for multimedia medical image database systems. In: Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges, pp. 52–55. ACM, New York (2001)
33. Kahl, C., Bttcher, K., Tschersich, M., Heim, S., Rannenberg, K.: How to Enhance Privacy and Identity Management for Mobile Communities: Approach and User Driven Concepts of the PICOS Project. In: Security and Privacy – Silver Linings in the Cloud. IFIP Advances in Information and Communication Technology 330, pp. 277–288. Springer, Boston (2010)
34. Pearson, S., Shen, Y., Mowbray, M.: A Privacy Manager for Cloud Computing. In: Proceedings of the 1st International Conference on Cloud Computing, LNCS 5931, pp. 90–106. Springer-Verlag Berlin, Heidelberg (2009)