User Centred Networked Health Care
A. Moen et al. (Eds.)
IOS Press, 2011

© 2011 European Federation for Medical Informatics. All rights reserved.
doi:10.3233/978-1-60750-806-9-497

Framework Model and Principles for Trusted Information Sharing in Pervasive Health

Pekka RUOTSALAINEN[a,1], Bernd BLOBEL[b], Pirkko NYKÄNEN[c],
Antto SEPPÄLÄ[c], Hannu SORVARI[d]
[a] *National Institute for Health and Welfare, Finland*
[b] *University of Regensburg, Germany*
[c] *University of Tampere, Finland*
[d] *Turku University, Finland*

Abstract. Trustfulness (i.e. health and wellness information is processed ethically, and privacy is guaranteed) is one of the cornerstones for future Personal Health Systems, ubiquitous healthcare and pervasive health. Trust in today's healthcare is organizational, static and predefined. Pervasive health takes place in an open and untrusted information space where person's lifelong health and wellness information together with contextual data are dynamically collected and used by many stakeholders. This generates new threats that do not exist in today's eHealth systems. Our analysis shows that the way security and trust are implemented in today's healthcare cannot guarantee information autonomy and trustfulness in pervasive health. Based on a framework model of pervasive health and risks analysis of ubiquitous information space, we have formulated principles which enable trusted information sharing in pervasive health. Principles imply that the data subject should have the right to dynamically verify trust and to control the use of her health information, as well as the right to set situation based context-aware personal policies. Data collectors and processors have responsibilities including transparency of information processing, and openness of interests, policies and environmental features. Our principles create a base for successful management of privacy and information autonomy in pervasive health. They also imply that it is necessary to create new data models for personal health information and new architectures which support situation depending trust and privacy management.

Keywords. Pervasive health, ubiquitous computing, privacy, trust, modeling.

1. Introduction

Information processing in today's healthcare takes place in closed environments where organizational trust and security is a rule. New service models such as Personal Health System (PHS) and ubiquitous healthcare use sensors, motes and surveillance systems to monitor data subjects (DS) in their daily living environment [1]. This means a jump from controlled and trusted environment to dynamic, uncontrolled and unsecure one. In spite of those changes these models are only extensions of today regulated and in many cases paternalistic healthcare paradigm.

[1] Corresponding author: Pekka Ruotsalainen, E-mail: pekka.ruotsalainen@thl.fi

A more revolutionary paradigm is pervasive health which takes part in ubiquitous information space. The pervasive health model tries to change today healthcare delivery model from doctor- and organizational-centric to person-centric, from acute reactive to preventive, and from sampling to continuous monitoring [2]. It integrates medicine, biomedical engineering, medical informatics, and ubiquitous computing [3]. Instead of focusing on eHealth services that healthcare professionals provide to patients, pervasive health is person-centric and person-driven. It is strongly targeted to make health and welfare management personal. Typical pervasive health services are location based services, pervasive access to health and wellness data, and lifestyle management [4].

Because pervasive health is not organization-centric, it enables a person to act as her own wellness coordinator and primary decision maker (with or without the help of any healthcare provider). Other unique features in pervasive health are:

- It enables the use of services which are not offered and controlled by regulated healthcare providers,
- Heterogeneous personal lifelong health and wellness related information together with rich contextual data is widely collected and used by stakeholders,
- Personal health and wellness information is not stored in today's regulated electronic healthcare records (EHRs),
- The data subject can set personal preferences regarding the use of her data, and,
- It uses ubiquitous computing for data collection, processing and sharing [4].

In this paper we use literature analysis to find major security and privacy risks which exist in pervasive health. We also demonstrate that the way privacy and trusted information processing have been implement in today's healthcare information systems cannot guarantee privacy and autonomy in pervasive health. Using analysis results and the developed reference model for pervasive health, we have formulated new realizable principles for trusted information processing and sharing in pervasive health.

2. Reference Model for Information Processing in Pervasive Health

Our reference model uses the concept of spaces (e.g. sub-systems, digital territories or bubbles), relations and polices (Figure 1).

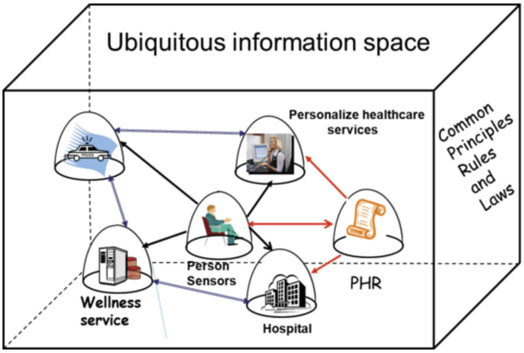
Ubiquitous information space
Personalize healthcare services
Common Principles Rules and Laws
Person
Sensors
PHR
Wellness service
Hospital

Figure 1. Framework model for information flow in pervasive health

Each space can have own business concepts, ethical rules, regulatory framework, context, and security and privacy policies [5]. Relations between spaces are dynamic without predefined trust. Any space can collect, process, store, and disclose health data. One of these spaces is data subject's personal space. Principles (rules, agreements, regulations and policies) define the way spaces communicate and process data. Health data can be distributed or it can be stored in the Personal Health Record (PHR). Information sharing between spaces is dynamic and context-aware. In such environment, the DS have problems to know whom they can trust, what the level of trust is, and what kind of data is collected, processed and shared by whom? It is also difficult to be aware of, and control, the secondary use of personal health data.

3. Information Content and Processing View

Pervasive health is characterized by heterogeneous information, dynamic number of stakeholders, and ubiquitous computing which seamlessly interconnects digital infrastructures into our daily life. It collects, processes, and distributes "any kind" of personal information and contextual data at any time. Pervasive health uses information about individuals that exceeds what today's organization-based EHRs can offer. It requires knowledge of individual´s normal functions in order to provide early detection of diseases, changes in functionality, and to offer pro-active prevention as well as personal health and wellness prediction services. This means that pervasive health requires information which covers person's whole life including data about personal behaviors, lifestyle, emotions, genealogical and genomic data, social data, data of psychological functionality, and data from environmental and body sensors. Rich contextual data and full or partial copies of the legal EHR might also be used. Those features mean that dynamic and context-aware trust and privacy management are needed.

4. Security and Privacy Threats in Pervasive Health

Ubiquitous computing used by pervasive health and features of information space generate many security and privacy threats which do not exist in today's healthcare systems and networks. It has been discussed already that there is no predefined trust between spaces in pervasive health. Furthermore, health data can be collected, processed, and communicated invisible to the DS, and contextual information can be easily misused. Dataveillance enables monitoring of person's activities and behaviors, and it is difficult to control the secondary use of data by multiple agencies. Ubiquitous computing generates digital footprints of all events. It enables privacy breaches by linking of multisource, heterogeneous and context-depending information. It has also unlimited memory.

5. State of Art of Data Privacy and Information Autonomy in Today Healthcare

Widely accepted principles for fair information processing include principles of withholdings, trusted usage, controlled dissemination and processing, transparency and security. Legitimate ground for processing is also required [6]. A typical way how those principles are implemented in today's healthcare information systems is shown in Table 1.

Table 1. Typical implementation of privacy principles in today healthcare.

Principle	Typical Implementation
Existence of personal privacy	Patients' privacy can be overridden in situations and purposes defined by national legislation.
Withholdings	Patients do not have right to control the content of their EHRs.
Trusted usage	Blind and organizational trust. Realized by security services. Trustfulness is seldom audited or certified.
Controlled dissemination	Patients' right to control dissemination is restricted by national legislation.
Transparency	Patient is not automatically aware which professionals or entities are processing her EHR and for what purposes. Patient is not aware of all disclosures of the content of her EHR.
Control over the creation, collection, processing and archiving of EHRs	Typically patients' have no right to those activities. Patients have limited or sometimes no control over processing of their EHRs inside healthcare organizations.

Table 1 show that today's implementations are based on blind trust and follow the manifestation of organization-centric and paternalistic healthcare model. At more technical level, security solutions used in today's healthcare information systems are organizational, reactive, and based on static rules. They are neither context-aware nor content-aware, and are targeted to be used in controlled environments with predefined rules. Even modern infrastructures developed for national healthcare information networks (NHIN) have adapted the models shown in Table 1. Based on the analysis of the previous chapters, it is clear that today's security and access control focused implementation models cannot guarantee trustfulness and privacy in pervasive health. Therefore newly formulated principles and information system architectures are needed.

6. Principles for Trusted Information Processing in Pervasive Health

Our proposal is that the DS have new rights and spaces/stakeholders have mandatory responsibilities covering collection, processing and sharing of health data. The DS should have rights to:

- Verify dynamically trustfulness of any space, and control the use of personal health information both inside spaces and between them,
- Be aware of all events and situations where health data is collected, processed, stored and shared, and
- Define situation specific, context-aware and granular personal policies regulating the processing and disclosure of personal health data.

Spaces/stakeholders have responsibilities to ensure:

- Transparency in data processing, openness of relationships between spaces, openness of their interests, policies and environmental and contextual features.

Our principles imply that the DS should not only be aware of the use of her personal health data but she also needs power to control how data is used, processed and shared.

7. Discussion

Our principles are not completely new. Some researchers have proposed patient controlled EHR/PHR and health data banks [7], [8]. Those proposals are limited to today's healthcare rules and to the use the predefined trust models. As our target is pervasive health without predefined trust, we have used privacy and trust frameworks developed for social web and ubiquitous computing as a starting point [9], [10]. From healthcare perspective, the adaption of our principles means a paradigm change which has big impact to services, to data models of the PHR and to information architectures.

Remaining challenges are both technical and political. The use of our principles can easily create a huge amount of personal policies. It is also difficult to manage and solve automatically policy conflicts between spaces without common security and privacy ontologies. In real life, some individuals do not have the ability or the willingness to use personal policies and verify trust. This all means that implementation of our principles will require the combination of personal, context-aware, dynamic and computer understandable security and privacy policies, trust verification, data encryption, notification services and capsulation of data and related contextual metadata. A Trusted Third Party service which can act on the behalf of the DS to manage trust seems also necessary. A big political challenge is to what extent business companies and governmental as well as professional organizations and health professionals have willingness to implement our principles.

Our further work focuses on ontologies for trust, privacy and wellness. Our principles should also be converted to a computer understandable policy language. We will also develop a security and privacy architecture which realize our principles.

Acknowledgements: We acknowledge the funding of the THEWS-project (Trusted eHealth and eWelfare Space) by the Finnish Academy of Science within the MOTIVE research program during 2009-2012.

References

[1] Kiefer S. Personal Health Systems (PHS) Overview and Research Trends, Fraunhofer Institut, Biomedizinische Technik, 2007, ec.europa.eu/information_society/events/phs.../phs2007-kiefer-s1a.pd.

[2] Arnrich O, Mayora J, Bardram G, Tröster B. Pervasive Healthcare Paving the Way for a Pervasive User-Centered and Preventive Healthcare Model, *Methods Inf Med* 49 1 (2010), 67-73.

[3] Bardram J, Pervasive Healthcare as a Scientific Discipline, Method Inf Med 47 3 (2008), 178-185.

[4] Varchney U. *ACM Communications*, December 2003, pp. 138-140.

[5] Beslay, L, Hakala, H. *Digital territory: Bubbles*. In Wejchert, J., ed.: The Vision Book, Brussels, 2005

[6] Wassernaar J. Privacy Rules, A Steep Chase For Systems Architects, www.w3.org/2006/07/privacy-ws/papers/04-borking-rules.

[7] Huda N, Sonehara N, Yamada S. A privacy management architecture for patient-controlled personal health record systems, *Journal of Engineering Science and Technology* Vol. 4.No. 2(2009), 154-170.

[8] Ball M, Gold J. Banking on Health: Personal Records and Information Exchange, *Journal of Healthcare Information Management*, Vol. 20, No 2. (2006), 71-83.

[9] Joshi A, Finin T, Kagal L, Parker J, Patwardhan A. Security policies and trust in ubiquitous computing, *Philosophical transactions of the Royal Society*, A (2008) 36.

[10] Langheinrich M. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems, www.inf.ethz.ch/~langheinrich.

Copyright of Studies in Health Technology & Informatics is the property of IOS Press and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.