ANTTO SEPPÄLÄ

Context-aware and Trust-based Personal Wellness Information Framework for Pervasive Health

■

ACADEMIC DISSERTATION
To be presented, with the permission of
the Board of the School of Information Sciences of the University of Tampere,
for public discussion in the Lecture Room Linna K 103,
Kalevantie 5, Tampere,
on April 16th, 2014, at 12 o'clock.

UNIVERSITY OF TAMPERE

ANTTO SEPPÄLÄ

Context-aware and Trust-based Personal Wellness Information Framework for Pervasive Health

Acta Universitatis Tamperensis 1924
Tampere University Press
Tampere 2014

ACADEMIC DISSERTATION
University of Tampere
School of Information Sciences
Finland

Cover design by
Mikko Reinikka

Distributor:
kirjamyynti@juvenes.fi
http://granum.uta.fi

Acta Universitatis Tamperensis 1924
ISBN 978-951-44-9420-8 (print)
ISSN-L 1455-1616
ISSN 1455-1616

Acta Electronica Universitatis Tamperensis 1408
ISBN 978-951-44-9421-5 (pdf)
ISSN 1456-954X
http://tampub.uta.fi

Suomen Yliopistopaino Oy – Juvenes Print
Tampere 2014

Table of contents

Abstract

The healthcare sector is currently facing many challenges, and technological innovations are changing the way health services will be provided in the future. One trend affecting health service provision is the citizen-centred care paradigm, whereby citizens are placed at the centre of care processes that allow them to take an active role. In the citizen-centred model, care provision is integrated and cross-institutional.

The objective of this dissertation is to further develop the citizen-centred care paradigm by integrating it with new aspects such as a holistic view on health and wellness and pervasive computing. The research domain is characterised as an open and unsecure environment, and solutions require heuristic and qualitative approaches based on creativity. The thesis therefore uses design science research as a guiding scientific framework specifically the build-evaluate approach to develop constructs and models. The empirical material consists of focus group interviews to support iterative development and the constant evaluation of produced artefacts. The thesis also employs use scenarios as means to analyse different aspects of the possible future, and a feasibility analysis considers the results.

As a result of this dissertation, a new vision is created for collaborative healthcare which supports citizen-centeredness and the distribution of service provision. A personal wellness information model is developed to describe a holistic view on health and wellness. Pervasive health is defined as a system, and its privacy and security threats are analysed to create a set of principles to ensure trust in the processing of personal information. This dissertation presents a new way of approaching the trustworthiness of information processing in pervasive environments by using context information as a basis for privacy management and presents a privacy management architecture based on trust information.

This dissertation introduces a vision of technology-enhanced future health and wellness care, whereby privacy management is dynamic and adaptable instead of the traditional static, risk-based thinking.

Acknowledgments

I express my gratitude to my supervisor, Professor Pirkko Nykänen, and the coordinator of the Trusted eHealth and eWelfare project, Research professor, emeritus Pekka Ruotsalainen, for the support and guidance received throughout the process. Their work and support have made this dissertation possible. I also wish to thank co-authors, Bernd Blobel and Hannu Sorvari.

I would like to express my gratitude to Emeritus Professor Michael Rigby and Professor Reima Suomi for carrying out the preliminary examination of this thesis and providing encouraging feedback. I offer my special thanks to Professor Harri Oinas-Kukkonen for agreeing to be my opponent in the public defense. I also owe my gratitude to all research subjects who participated in the empirical research. I would like to thank Domenico Pisanelli for sharing his thoughts and allowing me to present this research in Rome; Riitta Luoto for helping me with contacting research subjects; the participants of the eHealth doctoral student seminar, and the personnel from the School of Information Sciences.

I acknowledge the support received from the Academy of Finland. Most of the research presented in this study is part of the research project, Trusted eHealth and eWelfare Space (THEWS), funded by the Academy of Finland in the MOTIVE Research Programme during 2009–2012. The author also acknowledges the support received from the School of Information Sciences, and the Tampere Doctoral Programme in Information Science and Engineering (TISE) (2012-13).

I also thank my family and friends for their support.

Tampere, December 2013

Antto Seppälä

List of abbreviations

AAL	Ambient Assisted Living
APPEL	Adaptable and Programmable Policy Environment and Language
CPPL	Context-aware Privacy Policy Language
DICOM	Digital Imaging and Communications in Medicine
DS	Design Science
EHR	Electronic Health Record
EPAL	Enterprise Privacy Authorization Language
ER	Entity Relationship
EU	the European Union
HCI	Human-Computer Interaction
HIT	Health Information Technology
HL7	Health Level 7
ICD	The International Classification of Diseases
ICPC	The International Classification of Primary Care
ICT	Information and Communications Technology
IEEE	The Institute of Electrical and Electronics Engineers
IHE	Integrating the Healthcare Enterprise
IMIA	The International Medical Informatics Association
IS	Information System
ISO	The International Organization for Standardization
MeSH	Medical Subject Headings
OBO Foundry	The Open Biological and Biomedical Ontologies (OBO) Foundry
P3P	The Platform for Privacy Preferences Project
PHR	Personal Health Record
PHS	Personal Health System
RIM	Reference Information Model

SAML	Security Assertion Markup Language
SNOMED	The Systematized Nomenclature of Medicine
THEWS	Trusted eHealth and eWelfare Space –project
UMLS	Unified Medical Language System
WHO	the World Health Organization
XACML	eXtensible Access Control Markup Language

List of publications

This dissertation presents a summary of research documented in the following original publications, references to which are made in the text according to their designated Roman numerals.

Paper I

Nykänen P and Seppälä A. Collaborative approach for sustainable citizen-centred health care. In Wickramasinghe N, Bali RK, Suomi R, Kirn S (eds.) *Critical issues for the development of sustainable e-health solutions: Healthcare delivery in the information age*, 2012, Berlin: Springer Verlag, 115-134. Reprinted with permission from Springer.

Paper II

Seppälä A, Nykänen P and Ruotsalainen P. Development of personal wellness information model for pervasive healthcare. *Journal of Computer Networks and Communications*. 2012, 596749, 10 pages.

Paper III

Ruotsalainen P, Blobel B, Seppälä A, Sorvari H and Nykänen P. A conceptual framework and principles for trusted pervasive health. *Journal of Medical Internet Research*. 2012, 14(2), e52, 12 pages.

Paper IV

Nykänen P, Seppälä A, Ruotsalainen P and Blobel B. Feasibility analysis of the privacy attributes of the personal wellness information model. In Lehmann CU, Ammenwerth E, Nøhr C (eds.), *MEDINFO2013: Studies in Health Technology and Informatics*, 2013, IOS Press, Amsterdam, *192*, 219-223. Reprinted with permission from IOS Press.

Paper V

Ruotsalainen P, Blobel B, Seppälä A and Nykänen P. Trust information-based privacy architecture for ubiquitous health. *JMIR Mhealth Uhealth*. 2013, 1(2), e23, 15 pages.

Paper VI

Seppälä A, Nykänen P and Ruotsalainen P. Privacy-related context information for ubiquitous health. *JMIR Mhealth Uhealth*, 2014;2(1), e12, 12 pages.

1. Introduction

1.1 Background

The healthcare sector currently faces challenges associated with rising costs, increased demand, chronic diseases, uneven quality and misaligned incentives (1; 2; 3; 4). Europe is also facing an aging population, and the sustainability of healthcare has become more difficult because of the growing costs of social and health care, the increased number of retirees and the lack of medical professionals. These dynamics increase the intensity and variety of needed care services. Codagnone (1) has determined eight challenges that are likely to impact future healthcare systems: aging populations and other prevalence related trends (such as obesity), increasing income, consumerism and demand for equal and fair access, increasing capacity to cure, overshooting or mismatch in resource allocation, fragmentation and overspecialisation, inflation through unnecessary costs, and fat administration. These challenges highlight the need for more effective uses of resources (1; 3-7).

Healthcare is also affected by revolutionary technologies and evolutionary practices. Information technology and innovations have more recently played a much greater role in healthcare. Health information technology (HIT) has made significant progress and patients' clinical data has been, to a large extent, digitalised, and a lot of information is now available to clinicians (8). HIT will continue to affect healthcare in order to create new ways of providing health and wellness services. The accessibility and quality of healthcare services must be secured, possibly by innovative HIT solutions and new service models. eHealth has been a very important research area in the European Union, and during the last decades the EU has seen much potential in personal health systems (PHS) and in connecting citizens with healthcare networks (1).

Consumerism and citizen-awareness are relevant trends in healthcare. These trends suggest that citizens are aware of their health and wellness and want to choose which products and services they use and purchase. Consumerism leads to

more personalised services and choices (9-11). Healthcare is becoming more personalised as care, diagnostics and treatments will, in the future, be based on individual information (12). Healthcare delivery is widely seen to be transforming into citizen-centred care, that is, citizens are placed at the centre of care processes and play an active role in their own care (4; 5; 13-16). The starting point in this dissertation is a vision of future healthcare based on the citizen-centred care model with collaborative, distributed, and personalised health and wellness services. The focus of healthcare is on a person's overall health, wellbeing and functionality with prevention, early detection and proactive care.

The rapid development of HIT has initiated the concepts of pervasive healthcare and ubiquitous healthcare. These paradigms have been defined as an application of pervasive computing (i.e., ubiquitous computing, proactive computing or ambient intelligence) for healthcare and health and wellness management. The purpose is to make healthcare available anytime and anywhere (3; 17). The core of these paradigms is to integrate health technologies and concepts into everyday life (18; 19). The term, healthcare, has traditionally referred to strictly regulated and licenced activity, and therefore, in this research the term, pervasive health, has been used to emphasise the importance of activities, actors, services and providers outside the regulated healthcare domain.

1.2 Research questions and objectives

The focus of this research is on citizens, their personal wellness, personal wellness information and their personal information processing according to their own preferences in pervasive health. The key research questions are:

- What is the citizen-centred care paradigm, and what kind of technological vision is needed to support it?
- What is the information model for personal wellness?
- What are the challenges concerning trust, privacy and security with personal information collected in pervasive health?
- What rights and responsibilities should citizens and information processors have in pervasive health?

- What kinds of principles are needed in pervasive health for making information trusted?
- How are trustworthiness of information processing and citizens' rights to privacy ensured in pervasive health?
- What kind of privacy architecture is needed to support citizens' possibilities to control his/her privacy in pervasive health?

These research questions lead to five main research objectives:

1. To analyse the citizen-centred healthcare paradigm in the literature and to create a vision for future healthcare.
   - To look at how the citizen-centred care model is presented in the literature, how it differentiates from traditional healthcare, and what kinds of technological solutions exists.
   - To create a new, next generation and innovative view on collaborative health and wellness information space which can link service providers with citizens, thus enabling distributed health services and resources.
2. To create a high-level personal wellness information model that describes how citizens conceptualise their personal wellness.
   - To define what the concept of personal wellness means, what are the main components and concepts and what factors influence and characterise personal wellness and to define its scope and contents.
3. To define pervasive health as a system, to analyse its privacy and trust challenges and to define the principles for making it trustworthy.
4. To develop a privacy management architecture to help citizens to control their privacy and information processing in pervasive health.
5. To analyse what kind of context information is needed to enable trust in information processing and to enable citizens' rights to privacy.
   - To define what context information from information processing situations in pervasive health is needed to enable dynamic, situation-based privacy management.

1.3 Thesis structure and outline

This dissertation is structured as follows. Chapter one presents an introduction and describes the research questions and objectives. Chapter two presents the scientific approach and methods. Chapter three introduces the research domain by defining the concepts of privacy and trust, and describes the transition of healthcare. Chapter four analyses related research. Chapter five summarises the research papers with their main results. Chapter six discusses the results and considers the implications and usefulness of the research, reflects on the research and its limitations and presents recommendations for further research. Chapter seven presents the conclusions of this dissertation.

This research summary is based on six papers.

- Paper I presents the analysis of citizen-centred healthcare, its drivers and barriers as well as possibilities and ready solutions. The main contribution of Paper I is the vision for collaborative, sustainable citizen-centred healthcare.
- Paper II describes the development of the personal wellness information model. The main contribution of the model is the definition of the scope and contents of the personal wellness domain.
- Paper III extends the definition of pervasive health with a system model, and as a main contribution, presents a set of principles to guarantee the privacy and trustworthiness of information processing in pervasive health.
- Paper IV presents a feasibility study on the personal wellness information model and defined privacy attributes. The main contribution is the analysis on the applicability of privacy attributes with the personal wellness information model.
- Paper V describes what kinds of approaches are needed in pervasive health to ensure citizens' rights for privacy and to control their information processing. The main contribution is a privacy management architecture based on trust information. The developed architecture enables citizens to manage information privacy and set personal privacy policies.

- Paper VI describes the need for privacy related context information in pervasive health to ensure trust and citizens' rights to control their privacy. As a main contribution, it defines the context information that is needed to create context-aware privacy policies and to increase trust in the processing of personal information in pervasive health.

1.4 Author's contributions

The author's contributions to the original publications, I-VI, are as follows:

I. This article was a joint effort, and the author was responsible for writing the personal health sections and citizens' perspective on citizen-centred care and its current domains and drivers. He participated fully in the entire process of developing the future healthcare vision, and in the planning, writing and finalising the article.

II. The author designed the study and was the main person responsible for the empirical research, modelling and writing of the article. Throughout the process, the author received support and comments from the co-authors.

III. The author participated actively in extending the definition of pervasive health, creating the system model for pervasive health and developing the principles for trusted information processing. Throughout the research process, the author participated actively by sharing ideas and giving input and feedback to consecutive text versions.

IV. The author participated fully in the design and execution of the study and provided input and comments for the paper during the writing process.

V. The author participated fully in the development and design of the privacy management architecture, and the author presented ideas and gave input and feedback to all text versions.

VI. The author was the main person responsible for the design and execution of the research as well as drafting the various versions of the article. The author also integrated all contributions and suggestions and completed the final version of the article.

2. Research approach and methods

2.1 Research approach

The guiding scientific framework for this dissertation is the design science (DS) research approach (20; 21). DS research has become a widely accepted approach in information systems (IS) research (22), with publications of several journal special issues and conference workshops (23). One of the main reasons for the growing interest in DS research is that it focuses more on design aspects of IS research than the traditional behavioural oriented IS research (23). Although DS research has been discussed in the scientific literature since the 1990s (e.g., 20), it became a mainstream approach for IS research after the publication of DS guidelines by Hevner et al. (21, 23).

The DS research approach is a problem-solution focused framework where the main objective is to solve actual real-world problems by creating concrete artefacts or applications. DS research can be seen as a design process that produces innovative solutions. According to (21), DS research is suitable for problems which can be characterised by:

- Unstable requirements and constraints based on poorly defined environmental contexts,
- Complex interactions between the subcomponents of problems and solutions,
- Design processes and artefacts' tendency to change,
- Critical need for human cognitive abilities (e.g., creativity) and social skills (e.g., teamwork).

In this dissertation, I have followed the view and guidelines for DS research (21):

1. The DS research process should produce a purposeful artefact.
2. The research objective should be a solution for relevant business problems.
3. Design artefacts should be evaluated for utility, quality and efficacy.

4. Research should contribute to the areas of design artefact, design foundations, and/or design methodologies by solving an unsolved problem or improving known solutions.
5. The construction and evaluation of design artefacts should be done by using rigorous methods.
6. Design should be performed as a search process.
7. DS research should be communicated and presented effectively.

DS research is based on two processes, *build* and *evaluate*, which are performed iteratively to improve the quality of the design artefacts. The build processes can produce four types of artefacts — constructs, models, methods and instantiations (20; 21). Constructs, or concepts, form the vocabulary (i.e., language) of the domain. With constructs, designers can create a conceptualisation that describes problems and specifies solutions. Models are a set of propositions that define relationships between constructs, representing situations related to the problem or the solution. Thus, models can be simplified as a representation of how things are or should be. A method is a set of steps of how to perform a task, i.e., a process. Methods provide instructions on how to solve problems. Instantiations are working artefacts that implement constructs, models, and/or methods, demonstrating feasibility and enabling evaluation of an artefact for its intended purpose. DS research focuses on assessing the utility of the results and on fulfilling a real business need (20; 21).

2.2 Methods

In this dissertation, the DS research approach is the methodological framework which guides the research, and under it, different methods are applied. Focus groups, modelling, scenarios and a feasibility study are applied with a focus on building and evaluating constructs and models. Methods and instantiations from build and evaluate process are only considered and outlined in this research. The defined constructs and models create additional knowledge for the further advancement of pervasive health.

2.2.1 Focus groups

Focus group interviews form the core of the empirical component of this dissertation. Focus groups are suitable for situations in which existing knowledge is limited, research questions are very open and/or the domain is complex with many variables. The focus group is a method designed for group interviews where the emphasis is on communication and interaction within the group. The number of participants in a group may vary, but according to (24), the ideal size of a group varies between four and eight participants. The basic objective of focus groups is to generate data based on interaction and communication between participants instead of direct questions by the researcher. Focus groups are used to capture participants' knowledge and experiences. The group form helps participants clarify and explain their views, although sometimes, group dynamics may silence some participants or ideas (24; 25).

2.2.2 Modelling

In this dissertation, two types of models are created, namely, information and system. The aim of information modelling is to capture the information in a certain domain. To be able to use information properly, its meaning and structure have to be defined. Information models can be used to communicate information and to develop information systems which can manage and exploit this information (26). Information models can capture users' perceptions and understanding of system complexities (27). Information modelling can be conducted on three levels: physical, logical and conceptual (26). In this research, the focus is on the conceptual level of modelling. In conceptual modelling, the objective is to build a representation of real-world semantics in a certain domain (28-30).

Conceptual modelling can be used as a technique to analyse characteristics of a domain. Conceptual models are usually graphical models describing either static (e.g., things and their properties) or dynamic (e.g., events and processes) phenomena (31). A conceptual model is a tool for analysis in systems development, as it transforms the real-world into a model (28). With conceptual models, developers can create a common language for an application area, and communicate and reason

about the domain. Conceptual models define the concepts and the structure in the domain by defining the properties and relationships of the concepts in a formal or informal model (30; 32; 33).

System modelling in this dissertation follows the IEEE 1471 standard for architectural description (34). This standard provides a conceptual framework for describing systems architecture. Architecture provides fundamental organisation of systems, their components and relationships, in this case, the concepts and principles. Following this method, a conceptual level system model has been created to describe trust- and privacy-related concepts and their relationships in pervasive health. The idea of the model is to link these concepts to the research context of trustworthiness and privacy in pervasive health.

2.2.3 Scenarios

Scenario-based design techniques focus on projected systems usage. Scenarios are stories about people and their activities. They describe how people do things and how they can accomplish different tasks (35). As scenarios are used to project future behaviour, with them, designers can find new ways of doing things and even new things to do. Scenarios can be used to capture goals, entities, behavioural information (e.g., actions, activities, events) and the objectives and reasons for system usage. Scenarios usually have some sort of setting and a plot that may include several different actions and events, things that happen during activities, things that actors do or happen to them, changes in the setting, etc. Scenarios try to represent the use of the system and make it explicit, thus providing a framework for system design. Scenarios focus on activities and tasks, and with them, designers can analyse situations of use before the actual systems are used (35; 36).

2.2.4 Feasibility study

A feasibility study is an analysis of whether developed models or services are feasible for their intended purposes. Feasibility studies allow researchers to collect evidence on the feasibility of results before the actual implementation of the results (37). The feasibility criteria for a study are defined to satisfy the scope and

objectives of the research. Feasibility studies are a means to provide a proof-of-concept.

3. Research domain

3.1 Privacy and trust

Privacy refers to an individual's ability to control information about him/herself (38). It is a very subjective and context-dependent concept, as its shape and scope may vary between jurisdictions, cultures, economies, time and individuals (39; 40). Saltzer and Schroder (41, p. 1279) have defined privacy as "The ability of an individual (or organization) to decide whether, when, and to whom personal (or organizational) information is released." Westin (42) emphasises the importance of communication, and individuals', groups' and institutions' abilities to control when, how and to what extent information about them is disseminated. Skinner et al. (40) point out that privacy is a human right. According to (43), privacy is so dependent on the specific context that it is impossible to conceptualise it as a one-size-fits-all solution, and it should be regarded as a set of interests rather than a single, unambiguous concept.

Privacy is multidisciplinary by nature and is usually subsumed under ethics (43). It is often seen as a moral or legal right, and according to (44), it should be understood as the interest of sustaining personal space free from interference from others. Based on this, Clarke (44) has divided privacy into four dimensions:

- Privacy of the person
- Privacy of personal behaviour
- Privacy of personal communications
- Privacy of personal data.

According to (38) personal communication and privacy of personal data can be merged into the concept of information privacy.

Information privacy is one aspect of the concept, and it concerns access to identifiable personal information (43). Clarke (44) maintains that information privacy refers to an individual's claim that personal data should generally not be available to people or organisations, and that the individual should maintain a

substantial degree of control or influence over his/her data in the possession of other parties. Belanger and Crossler (38) point out that there are many definitions of information privacy, but usually with little variation in content, and that these definitions mostly include some sort of control or influence over secondary use of personal information. Secondary use refers to the use of information in a context or for a purpose for which it was not originally intended. Pavlou (45) summarises information privacy as maintaining control over personal information. Identity protection is another component of information privacy (40). Smith et al. (43) define four contexts of information privacy and privacy beliefs:

1. The type of information collected from individuals. This refers to contextual sensitivity or information sensitivity.
2. The sector using the information.
3. Political context (e.g., constitutional rights of self, government, freedom of press, and media), and
4. Technological applications.

Although the definitions of information privacy are relatively simple, it is a very complex concept, and it is studied in many scientific disciplines, e.g., law, economics, management, computer science (45). The subject of information privacy has gained considerable momentum in information systems research because of information digitalisation and new technological innovations such as social networking and virtual worlds (38). The internet, pervasive computing, big data, and other technological advancements increase the importance of information privacy as they enable better and more efficient processing, utilisation, combining and collection of information (38; 43; 45). Belanger and Crossler (38) emphasise the importance of developing new tools for privacy protection for citizens, groups and organisations as a research domain for design science.

Trust is closely linked to information privacy and is often seen as a strong predictor of an individual's willingness to share personal information (45). Schoorman et al. (46) emphasise that trust is based on relationships and the level of trust is an expression of how big a risk an individual is willing to take. Trust is about an individual's subjectively thought probability that an agent will perform according to his/her promises. Thus, trust relationships are based on beliefs (47). Further, Gambetta (48, p. 218) maintains that "trust (or, symmetrically, distrust) is a

particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action".

Based on Gambetta's definition, Abdul-Rahman and Hailes (49) identify three characteristics of trust:

1. Trust is subjective.
2. Trust is affected by actions we cannot monitor.
3. The level of trust is dependent on how our actions are affected by another party's actions.

Trust decisions are based on experiences and knowledge, especially in familiar situations (47). Trust and privacy are interconnected, and usually, the higher the value of trust, the lower the need for privacy.

3.2 Healthcare in transition

Technological innovations and demographic, social, organisational and financial challenges together propel changes to healthcare in order to improve quality, efficiency of care processes and patient safety. Traditionally, healthcare has been organised in an organisation-centric manner with static care processes. Typically, care is organised according to specialty or single interventions from the physician's point of view. Healthcare organisations are usually separate entities distributing primary care, specialised or secondary care and tertiary care with varied interests and objectives. Therefore, providers do not always work as a team, and for health professionals, it is not easy to capture the whole picture of a patient's health. Patients move between providers and health service levels, but there are communication lapses and delays in processes (5; 13; 14; 16). One potential future of healthcare is a transition towards citizen-centred care with a focus on the individual's complete health and wellness with all providers working together. The new healthcare paradigm concentrates on the health, functioning and wellbeing of people (50).

3.2.1 Citizen-centred healthcare

The basic assumption in the citizen-centred care model is that individual citizens are placed at the centre of care processes, and healthcare delivery is organised according to the citizen and his/her specific needs. The key issue is to enable citizens to take an active role in their own care processes. The citizen-centred care model emphasises a more holistic view on an individual's health and wellness, covering all aspects including diseases, prevention, early detection, proactive services, health promotion, and healthy lifestyle and behaviour (4; 5; 13-16; 51). In this context, Downing (12) describes future healthcare as preventive, pre-emptive, predictive, and participatory.

A new perspective on healthcare delivery as well as service models and collaboration between providers and citizens are needed to implement citizen-centred care. Healthcare should be citizen-oriented and organised to enable an interoperable and sharable network of services. Service networks and care processes should be multi-professional, decentralised, distributed, easily accessible and should support personalisation and actors outside healthcare organisations (12; 14; 16; 52-55). In the citizen-centred care model, the number of actors and actor types (e.g., providers, professionals, information systems, devices) involved in patient care increases.

Further, health information systems are distributed into own sectors or silos, and usually, data is fragmented and cannot be accessed when needed (3; 13). Organisations have their own information systems which are not all interoperable. Consumer products are stand-alone solutions and cannot be linked directly to health information systems because of legislation, accountability and possible problems with data integrity and trustworthiness. New tools and shared care management are needed to guarantee communication, information sharing and co-operation throughout the care process to ensure dynamic and integrated services (8; 14; 16; 55). Access to real-time, reliable and secure information is critical in order to justify decisions. Collaborative environments are an opportunity for healthcare organisations as they enable communication with stakeholders, aggregation of information and leverage collaboration (56- 58). Collaborative environments and social media have the potential to bridge the information, knowledge and collaboration gap in healthcare services and usage (59; 60).

Citizens are aware of their own health and wellness, are willing to participate in their own care and expect and demand more than ever from health services (4; 9; 10). Citizens' roles are transforming from passive patients to active consumers who are responsible for their care (12; 13; 53). This phenomenon of active citizen participation has been defined as citizen empowerment (4; 13-15; 53). As care services are fragmented, citizens need to act as care integrators who are responsible for the completeness of care (13). Citizen empowerment is a potential tool for cutting costs and for improving the quality of healthcare by moving responsibilities to citizens. It also improves prevention possibilities and wellness maintenance (4; 9; 54; 61-63).

Citizens are nowadays capable of sharing their personal information on the internet with different social media services, and health and wellness management applications (64). High quality information and communication is needed to empower citizens and to improve decisions and choices (3; 9; 65). Healthcare providers should open up and establish communication and collaboration with citizens to guarantee better information about their personal health and wellness (4; 14; 16; 52-54).

According to the World Health Organization (WHO) (61), 70-80% of expenses in healthcare emanate from chronic diseases, and improved medical care is decreasing the mortality rate of several chronic diseases (66). Seven leading risk factors – high blood pressure, tobacco, alcohol, high blood cholesterol, overweight, low fruit and vegetable intake and physical inactivity – account for almost 60% of the disease burden in Europe (61). Based on these risk factors, it can be understood how important it is to see health in a more complete and holistic manner, and how crucial it is to support citizens' actions outside the clinical world. Since risky lifestyles are a major cause of many chronic diseases (66), the future aim should be on preventive care, health promotion, early diagnostics with continuous monitoring, better control of non-communicable diseases and proactive and multidisciplinary services to provide citizens with a more complete well-being and improved quality of life (2; 4; 12; 19; 52; 53; 61).

3.2.2 A holistic view on health and wellness

The WHO has defined health as "a state of complete physical, mental and social well-being and not merely the absence of disease of infirmity" (67). This definition shows that as early as 1948, the WHO acknowledged the holistic view on health, and that it should be more than just treating diseases. According to (63), the problem with the WHO's definition is that it basically makes every person with a disability or a chronic disease definitely ill because of the absoluteness of the word 'complete' in relation to well-being, and that the definition minimises the meaning of capability to cope autonomously and function with changes in physical, emotional, and social challenges. Huber et al. (63) claim that health should be viewed as the ability to adapt and to self-manage. Rigby (11) states that health is far more than just the product of healthcare services; it is a personal state, a very unique state for every individual, and all sorts of activities and factors are important for its maintenance.

The concept of health can cause confusion as it can be understood to mean a state free of diseases, or a stable physiological function that focuses on medical well-being. The wellness concept has been used to refer to a broader view on the health and well-being of people. Wellness is a multi-dimensional concept covering a person's general functioning as a whole and taking into account physical, social and psychological aspects (68; 69). It is currently being studied in many scientific disciplines, e.g., medicine, public health, occupational health and mental health (68).

The literature contains several context-specific definitions of wellness. In many of them, wellness considers a balanced state of a healthy body, mind and spirit creating a harmonious feeling of complete wellness (50; 68-73). Wellness can be defined as a high-level concept integrating multiple domains related to general health and well-being (72-75), including lifestyle, behaviour, culture, beliefs, experiences, etc. (68; 69; 71; 73; 75; 76). The view on wellness may vary between individuals depending on age or culture, and it focuses on an individual and his/her specific needs.

Health promotion, prevention and progress toward better functionality are tightly linked with wellness (50; 75; 77) and are major trends in different media (78). Many magazines, TV and websites focus on health and wellness to promote better lifestyles and behaviour choices including exercise, healthy nutrition, limiting alcohol consumption, smoking cessation, adequate sleep, stress management, etc.

Also the line between pharmaceutical and wellness products is wavering (78). Self-management is closely related to wellness and suggests that citizens are responsible for the day-to-day management of their wellness activities, e.g., exercise and chronic disease management. Self-management aims to help maintain wellness by medical management (e.g., medication, special diet, and inhaler use), maintaining or creating meaningful behaviours or life roles and managing the emotional effects of chronic conditions (79).

3.2.3 Technology enhanced health and wellness

The availability and rapid development of ICT and HIT, such as pervasive computing, big data, internet of things, sensors, motes and ambient intelligence, are shaping future healthcare delivery. Traditionally, healthcare has been highly institutionalised and regulated, and services have been provided in controlled environments. With today's technological innovations, it is possible to transform the nature of healthcare into a citizen-centred, personalised and distributed framework, and services can be offered and information can be processed anytime and anywhere (3; 18). This creates challenges for privacy, trust and security as services can be offered in dynamic, uncontrolled and unsecure environments.

The key point in technology enhanced personalised health and wellness is to enable improvements with better prevention, earlier diagnostics, reducing costly later stage treatments and personal information based care. Technology also enables better pharmaceutical products and improves understanding of large-scale public health issues (e.g., microbes, chemicals and other harmful agents) with larger databases and genomic information (12). Atkins and Cullen (80) have identified nine trends for future HIT:

1. Connected health enables collaboration with providers and patients.
2. Controlling personal health data will be in the hands of the patients.
3. The amount of information available will be huge and a large portion is provided by the patients and their personal systems.
4. HIT will ease the efforts of promoting and assisting changes of behaviours into healthier.

5. Health data is centrally aggregated, and this will enable customisation of information visualisation based on the needs of patients and professionals.
6. Standardisation of data will enable assessments of larger datasets covering even entire populations in real time.
7. Personal information can be compared to selected population data.
8. Big data will enable real-time queries to help in diagnostics and therapeutic decisions and in the development of new clinical decision algorithms and tools for clinical care.
9. Improved access and documentation of national datasets for researchers.

There are tools that help citizens manage and maintain their personal wellness. These tools enable citizens to collect their own data from different information sources, reflect on their wellness, support healthier living and behavioural changes, collaborate between different actors and stakeholders and share their own personal information. There are extant solutions that support behaviour, exercise and wellness management, measuring and monitoring devices and sensors (e.g., blood sugar and pressure, ECG, skin temperature), ambient assisted living (AAL) and smart home systems supporting people at home (62; 81-88).

One suggested, and already existing, solution is the personal health record (PHR). PHR differs from typical health information systems because it is created for citizens' needs. PHR is not considered a substitute for legal electronic health records (EHR) and will not affect the legal obligations of healthcare providers (51; 89-92). PHRs are seen to support citizen empowerment and make health and wellness information available when and where it is needed, hence improving the quality of care and lowering costs (65; 91- 94). The scope, nature, functions, users and use contexts of PHR may vary between solutions, but usually, PHR is considered to enable access and the possibility to manage, control, collect and share personal health and wellness information and may include decision support to ease citizens' actions in managing and maintaining health and wellness. Information content is usually described as lifelong and cross-institutional, thereby enabling an integrated view (10; 89-93; 95).

Information systems and computing environments tend to be widely distributed. Notwithstanding, most systems and devices communicate in a non-standard manner and are not semantically interoperable. According to Bates and Bitton (55), current

EHR solutions lack capabilities to enable shared care and care transitions. Standards for interoperability and data transfer between EHRs and consumer systems are limited (4; 90). Information systems need to be able to share information and to make queries and requests, knowing that there is shared understanding of the meaning of information, i.e., semantic interoperability. To achieve this, common information models are needed to cover the domain of health and wellness. Based on the models, a personal wellness ontology needs to be created. Ontologies can be used to create shared understanding among all participants and to enable sharing of heterogeneous information (96; 97). Without interoperability, health and wellness information will remain fragmented in isolated silos, no real value will come from the huge information resources, and citizen-centred care will not be achieved. The lack of common understanding will not just hamper interoperability; it will also create security and privacy vulnerabilities (98).

4. Related research

4.1 Personal health and wellness information

In the field of health and biomedical informatics, there are several classification systems and ontologies (e.g., SNOMED, OBO Foundry, Gene Ontology, MeSH, UMLS, ICD, ICPC), standards for interoperability (e.g., HL7, DICOM, IHE), electronic health records (e.g., ISO 18308, EN 13606), and information models (e.g., HL7 RIM, ISO 13606). These have been developed mainly for traditional healthcare providers and their records, processes and needs. Thus, they are designed to satisfy the needs and views of organisation-centric healthcare, and therefore, they do not fully support a paradigm shift to citizen-centred care and a holistic lifelong view with a focus on citizens and their specific needs.

From a citizen's perspective, there are some wellness models, for example, developed in clinical and counselling psychology (99), which describe the components of a more complete wellness. Els and De La Rey (99) conceptualise wellness as consisting of six life domains: family and social interactions, work, spirituality, emotionality, intellectuality and physicality. Moreover, Sweeney and Witmer (100) develop the Wheel of Wellness model in which they recognise factors influencing healthy living, quality of life and longevity, which are connected, and change in one area can affect others (70; 101). Myers and Sweeney (70) then create a new model, the Indivisible Self, based on the Wheel of Wellness. It is based on five factors and their sub-factors:

- The Essential Self: spirituality, self-care, gender identity, and cultural identity,
- The Social Self: friendship and love,
- The Coping Self: realistic beliefs, stress management, self-worth and leisure,
- The Creative Self: thinking, emotions, control, positive humour and work,
- The Physical Self: exercise and nutrition (70; 101).

In this model, an individual's wellness and behaviour are affected by contextual factors: local (family, neighbourhood and community), institutional (education, religion, government and business/industry), global (politics, culture, global events, environment, media and community), and chronometrical (perpetual, positive and purposeful). All components affect and interact with each other, thus creating a holistic model of wellness (70; 101).

Further, Saylor's (102) Circle of Health model describes a holistic view on health. It represents both body and mind dimensions and defines health as optimal function, well-being, and quality of life. The model is divided into two components: activity and performance and renewal and recovery. Activity and performance include the following concepts: energy, strength, fitness, stamina, happiness, enjoyment, satisfaction, growth and development, occupational and/or social role, and performance. Renewal and recovery consist of rest, relaxation, peacefulness, nourishment, social support, sense of purpose and meaning, balance, adaption and resiliency.

Kirsten et al. (72) later create an ecosystemic approach to health, well-being and wellness based on two assumptions:

1. Humans are whole, complete individuals with some distinguishing attributes (holistic view on health).
2. Health, well-being and wellness are multi-dimensional and multi-disciplinary.

The model has three elements, contexts or domains which describe the functioning of a person (biological, psychological and spiritual) and two outside contexts (ecological and metaphysical). This approach sees holistic health and wellness as a continuous, dynamic and lifelong process where people, their health and wellness, and contexts are distinguishable but inseparable.

These models acknowledge the holistic and more complete idea of health and wellness, including more than just physical health or absence of disease. The models show that wellness is strongly dependent on external contexts and the importance of balance and harmony between different factors of health and wellness. Although wellness is studied in many scientific areas, its contents and boundaries have not been properly defined. Most research on wellness has focused on measuring or assessing wellness. Wellness models developed in clinical and counselling psychology are very high-level descriptions of the domain, and there is no real consensus on what personal wellness is and what are its more detailed components.

Overall, there is a lack of knowledge about personal wellness, its boundaries, content and scope. Also, existing research has not focused on information systems development.

4.2 Context information and context-aware computing

Context-awareness is a crucial element for enabling pervasive computing and services (103). A widely cited definition of context has been presented by Dey and Abowd (104, pp. 3-4): "Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves". Based on this definition, context information is any information that is relevant for information processing in a given situation. Information can be about the situation itself, an entity (e.g., user, device) participating in the situation, or the environment where the situation occurs. Therefore, context is usually talked about in relation to something that exists. Chen and Kotz (105, p. 3) further define context as "the set of environmental states and settings that either determines an application's behaviour or in which an application event occurs and is interesting to the user".

Moreover, Chen et al. (106) define context as information about a location, its environmental attributes, the people, devices, objects and software agents. It may also include system capabilities, services, activities and tasks performed by people or computing entities, and their situational roles, beliefs and intentions. According to Dourish (107), context and content cannot be separated. Context cannot be an external description of the setting as it arises from the activity itself. Hence, Dourish (107) claims that context is a relational property between objects and activities, and the scope of contextual features must be defined dynamically. Dourish (107) emphasises that context is an interactional problem and does not describe a setting; it is something that people do. Soylu et al. (108) further define context information as information and its relations that enable behaviour modification. The usage of information defines whether it is context information, and therefore, computational entities have to define the scope of context information themselves.

Dey and Abowd (104) divide context into location, identity, activity and time. Dey et al. (109) maintain that three of the most relevant entities whose contexts should be assessed are places, people and things. Places are geographical places; people can either be individuals or groups and co-located or distributed; things can be either physical or digital objects. Soylu et al. (108) place context into user, device, application, information, environmental, time, historical and relational categories. Brooks (110) has also introduced a context quintet, which needs to be analysed when assessing context, that is, who, where, when, what and why. These questions need to be answered to properly understand context. Hervas et al. (111) have further developed the context quintet by introducing a two-dimensional taxonomy with a second dimension consisting of user, environment, service and device.

Soylu et al. (108) have recognised two types of context information: direct and indirect. Direct information has to be sensed or defined. Indirect information is reasoned from direct information. Context information can also be either dynamic or static. Static information does not change over time, while dynamic information is highly dependent on changing parameters such as location or age (108; 112). Dynamic information is crucial because situations, entities and environments may change. Space or spatial information is an important dimension of context and Bettini et al. (113) believe that most context-based definitions emphasise space as a vital aspect. Schillit et al. (114) therefore conclude three important aspects of context:

1. Where the individual is
2. Who the individual is with
3. What resources are nearby

These aspects are clearly linked to the entity's location and environment. Spatial context information can be used to reason about location and spatial relationships with objects (113).

In order for pervasive computing to be minimally intrusive, it has to be context-aware (115). To enable this, context information has to be perceived, represented, processed, understood and reasoned. Context information cannot be properly used unless it has been modelled. Several context modelling and reasoning approaches have been developed to support context-aware application development. The use of proper context information modelling formalism improves the maintainability and

evolvability of context aware applications and reduces their complexity (113). According to (109), context information can be used for three main purposes:

1. Presenting information and services to a user or using context to propose actions to be performed.
2. Execution of a service automatically on behalf of the user.
3. Applications can tag context to information for later retrieval.

Context-awareness has been widely researched in the human-computer interaction (HCI) field (104; 112; 116; 117). According to Soylu et al. (108), context-awareness refers to adaptability. Thus, applications and systems are able to perceive their surroundings and environment and exploit this context information to react and adapt their behaviour to different situations autonomously. Context-aware systems are able to provide services and information for users by exploiting context (105). Chen and Kotz (105) have divided context-awareness into two types: active and passive. Active context-awareness means that applications automatically adapt to discovered contexts by changing their behaviour. Passive context-awareness means that applications present the new or updated contexts to users or make contexts persistent for later retrieval.

Although the importance of context-awareness is accepted, and it is researched widely in the HCI domain, Addas (116) emphasises that deeper and more systematic research on context is needed. In his (116) review of the past 30 years of research in HCI, he discovers that most research has focused on user and technology interaction. The two other aspects, task context and social/organisational context, have not been widely researched. Also, research has mostly focused on the individual level, and on some level, has ignored cross-level interactions. According to Addas (116), systematic research is needed to understand the various mechanisms by which the context can shape the underlying HCI phenomena.

4.3 Pervasive health research

Pervasive health constitutes research in pervasive computing, including collaborative, context-aware, embedded, mobile, proactive and sensor systems (19). Pervasive health uses these technologies for continuous monitoring, proactive and preventive services, early detection of diseases and ubiquitous access to health

information (18; 19). One of the key enablers of pervasive health solutions is context-awareness (118). This means that applications are able to perceive different contexts (e.g., location, physical activity) and process this information and make decisions based on it. Viswanathan et al. (118) have summarised three relevant characteristics of pervasive health:

- Collection of vital signs continuously and pervasive,
- Real-time access and procession of monitoring data and deriving meaningful physiological parameters,
- Data- and patient-centric context-aware decision making.

The number of actors and information sources in pervasive health is increasing, and it is possible to collect and process all kinds of data by using intelligent sensor networks and measurement and monitoring technologies (3; 4; 17; 18). The amount of data and information available in the future will be almost unlimited, and it will overcome the content and capabilities of the current EHRs and other health information systems. Monitoring and lifestyle data enables services to be proactive, preventive and capable of early diagnostics (3; 18).

Pervasive health can include services provided by regulated healthcare providers, devices or computational entities, different wellness companies and citizens own activities. Usually, the goal of pervasive services is to improve and monitor citizens' lives and functions through pervasive computing applications. In their review, Orwat et al. (119) point to 67 pervasive applications in healthcare, with 72% of these supporting patients, 51% nurses and caregivers and 54% physicians. Altogether, 63% of these systems aim to improve prevention and care, 12% support therapy and rehabilitation and 39% aim at organisational improvements (e.g., improved documentation or process automation).

Sensors and devices enable monitoring and measuring citizens' activities (e.g., physical activities, vital signs, emotional and mental functions), behaviours and risky situations and proactive and personalised services, support for independent living and home care and detection of emergency situations (e.g., falls, seizures, blood glucose level) (see e.g., 6; 83; 84; 118-121). Pervasive services enable citizen-centred care by using personalised health status, body sensor networks, monitoring, decision support and reminder applications (see e.g., 118; 122-128). Context-aware pervasive technologies can also be used in hospital environments to help hospital work and processes by personalising services for medical professionals by location,

time and social context (129). Context-aware services in hospitals have been experimented to improve patient record management, communication between professionals and information sharing with context-aware equipment (122; 130).

Atallah et al. (6) have identified five possibilities of pervasive sensor technologies in tackling problems faced in healthcare:

- Remote and continuous monitoring of chronic and infectious diseases,
- Allowing earlier release of post-operative patients from expensive healthcare environments by observing them at home,
- Providing techniques to understand aging and supporting elderly care management,
- Large-scale monitoring of environmental changes and the impact of urbanisation,
- New innovative techniques for maternal and neonatal care.

4.4 Privacy and trust in pervasive health

Different aspects of pervasive computing – such as continuous monitoring, location and movement tracking, smart spaces, and intelligent systems with capabilities to create patterns of human behaviour and other knowledge about people – create severe possibilities for privacy breaches (115). This very personal information has to be collected and processed to enable pervasive services, but its usage has to be strictly controlled, and users should be able to trust the pervasive infrastructure. Without proper privacy controls, pervasive computing may not reach its full potential. Privacy is a personal and context-dependent concept, and deciding whether privacy is good or bad is a primarily qualitative opinion. Therefore, it is more useful to measure the level of privacy or its attributes. Privacy metrics can be used to decide how systems comply with privacy preferences. With them, objective assessments can be performed on the privacy level of a system in order to distinguish privacy-aware applications that comply with good privacy from bad privacy applications (131).

Pervasive computing requires systems to be open and dynamic because they cannot pre-identify participants, as participants may change regularly (98). Collaboration is necessary in open, dynamic and distributed environments, such as

pervasive health, where multiple systems work together to achieve goals, utilise resources and perform tasks. In these kinds of environments, it is necessary for systems to know which entities they should or should not interact with (132). For instance, traditional authentication or role-based authorisation security and privacy management are not suitable in pervasive computing because simply identifying oneself is of no use in an open environment without central control and predetermined users (98; 133). Accordingly (see 98; 133; 134), the security and privacy architecture and decisions should be based on trust and its attributes.

Another component, computational trust, is about making intelligent agents trust each other in heterogeneous and distributed multisystem environments and enabling the delegation of tasks between trusted agents (135). Krukow et al. (136) define computational trust as an abstraction adapting the human concept of trust. It supports computational agents in decisions concerning unknown, uncontrollable and possibly harmful entities in a context which lacks reliable information and which makes traditional techniques useless. As such, computational trust is more than just access control; it is about decision making in unforeseeable environments with unforeseeable participants.

Introducing trust into multisystem environments may reduce unnecessary communication, improve decisions based on an evaluation of the trustworthiness of another system and complement traditional security measures (e.g., encryption, authorisation and authentication) (135). There are several trust models with different parameters developed for calculating trustworthiness (e.g., 46; 133; 135; 136). Trustworthiness is a perception of confidence in the reliability and integrity of a trusted party (137). According to (137), several researchers have agreed on three main elements of trustworthiness: ability, benevolence and integrity. Ability is self-evident, but benevolence is defined as the extent to which the trustor believes that the trustee is willing to do good things instead of maximising profits. Integrity concerns honesty and sincerity.

One key concept in this dissertation is policy. Policies are used to manage security, trust and privacy with explicitly defined and represented constraints and rules to control the behaviour of computational system. Traditionally, policies have been used in organisations to control security, but lately, they have also been introduced in privacy protection (138). With policies, data subjects can control how their information is processed, used or shared. Policies describe what entities are

allowed or constrained to do in a certain context (98; 139). Policies can be attached to data to ensure that data is processed in a manner that is compliant with the policy, a technique called sticky policy (139). Several languages have been developed to represent policies in human-readable and computer-understandable formats e.g., APPEL, P3P, EPAL, XPref, REI, SAML and XACML (140).

In pervasive computing, privacy management should be dynamic and be able to adapt according to context information and how it affects privacy (141, 142). In pervasive environments, there are multiple changing entities, and therefore, access control has to be dynamic and based on context information which enables the dynamic management of rights (142). While there is research on context-awareness and privacy, much of it focuses on protecting the privacy of context information i.e., protecting privacy in context-aware computing, and does not really consider using context of information processing as a basis for privacy protection (see e.g., 143-149).

Some context-aware privacy solutions exist and usually seem to focus on capturing the context of a user or a certain actor in a predefined situation and using that information to adapt privacy preferences. Schaub et al. (141) have developed a privacy context model in which they focus on privacy relevant context information. In their model, they identify three privacy aspects of context: the user, and his/her environment and activities. The user aspect is about his/her privacy sensitive items (e.g., information or action of an entity in a user's physical proximity). The user's environment is about his/her current location and can contain virtual and physical entities and the user's activities in a given situation. Change in any of these contexts can have privacy implications which require privacy decisions or adjustments in privacy settings. This model tries to take account of information, physical and territorial aspects of privacy.

The EnCoRe project has developed an architecture to control processing of personal data and enforcing privacy (139). Their architecture uses sticky policies, privacy-aware access control and obligation components to enforce users privacy preferences when data is accessed. In their solution external workflow manager tracks and monitors data flows within and between organisations to ensure that person's privacy preferences are followed. Systems willing to process data fully

have to be the EnCoRe compatible. If a system does not comply with the EnCoRe data might not be accessed to full extent.

Salah et al. (150) propose trust management systems architecture. The architecture calculates a trust score from monitored and collected trust aspects. Faravelon et al. (142) sees that privacy should be solved in the access control level. They propose a model-driven approach where privacy design and execution levels are separated. At first, they have developed a privacy meta-model and based on the model they define an architecture and how to implement it. The architecture presents a set of components to enforce access control and to check compliance with policies.

Behrooz and Devlic (151) present a context-aware privacy policy language (CPPL), whereby policies are set for different situations and the requestor can be specified according to his/her identity or social relation to the person. In CPPL, situations and privacy principles are defined separately. Blount et al. (152) introduce a context-dependent privacy policy model. In their model, privacy policies contain a field context which can include a set of contextual constraints that have to be satisfied for the policy to be effective. This information describes the subject or the requestor.

Ghosh et al. (153) present a semantic policy-based system which can constrain information flow by reasoning with a user's dynamic context. Their solution enables protecting the privacy of smartphone users at runtime instead of predefined user input. Corradi et al. (154) propose a context-based access control middleware that can dynamically determine the context of a mobile user, and permissions are associated with the contexts instead of typical identities or roles. Their solution allows system operators to specify access control policies and users to create their own privacy policies and to control the disclosure of personal information in a new context. This middleware supports physical and logical contexts, that is, physical contexts identify physical spaces and logical contexts identify states of both physical contexts and entities (users and resources). These states can depend on logical properties, e.g., temporal conditions, availability, activities or device characteristics.

Privacy is seen as the biggest obstacle for the widespread implementation of pervasive computing technologies due to its potential for abuse and the fear of not being able to control surveillance and information processing (143). Recently, however, some researchers have used the term privacy paradox, that is, while people

are concerned about privacy risks and breaches, they continue to share their lives, pictures, and information in different social networks (155). The wide coverage and huge usage of social networks clearly demonstrate that people are ready to share their information in computer systems, although some data such as medical records and financial data are found to be more sensitive than demographic characteristics, purchase behaviour or lifestyle data (155).

In the context of this dissertation, information privacy, trust and trustworthiness are key issues affecting the research and produced artefacts, as personal health and wellness information is, by law, highly confidential. Personal information should be protected from unauthorised use, secondary use, access, processing, disclosure and dissemination.

4.5 Summary of related research

The transition of healthcare has meant that some services are being moved outside the regulated healthcare environment. Service provision has traditionally been organised from the physician's perspective, and now, citizens' role is being transformed from being mere patients to active participants in their care. Also, current information systems are not all designed to handle the increasing amount and variety of health and wellness information. For example, electronic health records are not designed to support a complete, lifelong, cross-institutional view on health and wellness. To support the future development of healthcare, new tools and solutions are needed to ease the management of personal health and wellness information over organisational boundaries and enable collaboration between citizens and their personally selected providers.

There is a lot of research focusing on interoperability standards and the modelling of medical terms and concepts to support regulated healthcare, however, research on citizen-focused personal wellness, including information created outside provider networks, remains limited. There is no agreement on the knowledge basis of personal wellness in terms of covering a lifelong and holistic view on health and wellness information. Personal wellness has mainly been studied from a measurement or assessment point of view. These studies do not support the development of new computational tools and information systems. In order to

support the creation of a personal wellness ecosystem, and interoperability between different computational entities, the scope and contents of personal wellness have to be understood.

Pervasive computing and other technological innovations are shaping the future of healthcare. Technology is enabling almost unlimited possibilities for information processing and the creation of new pervasive services to automatically and autonomously manage personal wellness. This also creates serious privacy risks and a possibility to monitor and track citizens' location, movement, activities, vital signs and even emotional states. Pervasive health applications and wellness approaches do exist, and the type and amount of information and continuous monitoring of people require new ways of protecting privacy. Information processing environments are open and dynamic, and traditional privacy and security solutions were not designed to accommodate these features.

Citizens need means for ensuring their privacy, and privacy and trustworthiness are seen as main questions hindering the implementation of pervasive technologies. These issues are acknowledged in many scientific articles, and it has been proposed that privacy management should be dynamic and capable of adapting to different situations. The promises of pervasive health can only be fulfilled if privacy issues and the trustworthiness of information processing can be adequately solved within applications and systems. Although, the importance of privacy and limitation of traditional security approaches are widely acknowledged, it seems that trust based and architectural approaches for privacy management have not been really considered and most existing solutions try to fulfil privacy requirements with access control. Also research on context-aware privacy solutions is still limited and mainly focuses on single user contexts or some activity. What context information needs to be captured from information processing situations has not been widely studied. Thus, an approach of using situational information as a basis for privacy management has not yet been thoroughly considered.

5. Research results

5.1 Vision for collaborative healthcare

A next generation, semantically enriched, collaborative health information space has been envisioned in paper I (see Figure 1.). It is based on two collaborative virtual health spaces:

1. Regulated and legally controlled provider-side information systems (e.g., EHR).
2. Citizens' personal health space (e.g., PHS and PHR).

A collaborative information space covers all stakeholders, regulated healthcare providers, health professionals, patients, citizens and other interested parties. In order to support collaboration, the information space enables dynamic, effective information combining and sharing, and easily and safely accesses distributed health resources anywhere and anytime.

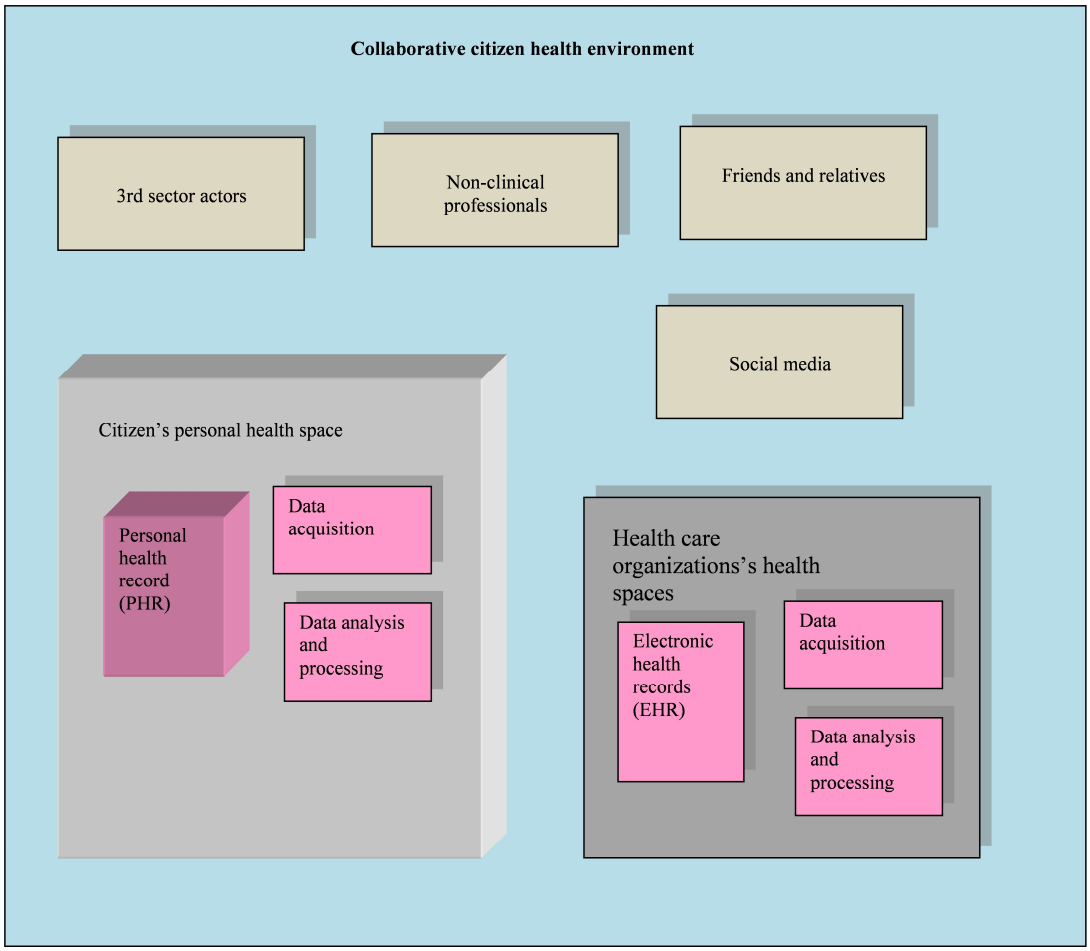


Figure 1. Vision on collaborative, sustainable citizen-centred health

Citizens are in complete control of their personal health spaces, and management and maintenance is mainly done by themselves. Citizens can select tools that are accessible and suitable for their situation and purposes. Providers control their own health spaces which contain legally regulated patient health data collected and registered by health professionals during citizens' care episodes and visits. This space is designed for the purposes of healthcare organisations like care documentation and support and administration. Providers' health spaces and information processing are legally regulated. Regulations lead to data transfers being mainly one-way, that is, citizens can copy or link their information from health providers' health spaces into their own health space, but they cannot transmit data registered by themselves directly onto health providers' spaces. However, citizens can enable health providers with access to their health spaces.

Future healthcare delivery will be collaborative and participatory. Health services are based on information, information systems and a community of actors surrounding a person's health and wellness. This vision supports shared and collaborative approaches to service provision, and defines a platform which supports communication, interaction and sharing of information. The citizen-centred care model and new tools for communication and collaboration enable citizens to take an active role in their own personal health and wellness and enable the creation of more personalised services which are available anytime and anywhere.

5.2 Personal wellness information model

The high-level personal wellness information model (Figure 2.) is based on a literature analysis as well as empirical research (II). The aim of the personal wellness information model development is to define the scope of the domain and present the related concepts, characteristics, relationships, and contextual aspects. The development, along with a literature analysis and empirical research, has resulted in a view on personal wellness as a basis for modelling. The view is composed of five internal components: lifestyle, emotional and mental wellness, occupational wellness, healthcare and physiological wellness. These components are surrounded by two external contexts: social networks and environment. Social networks focus on the social relations of a person, and environment describes both physical and digital environments.

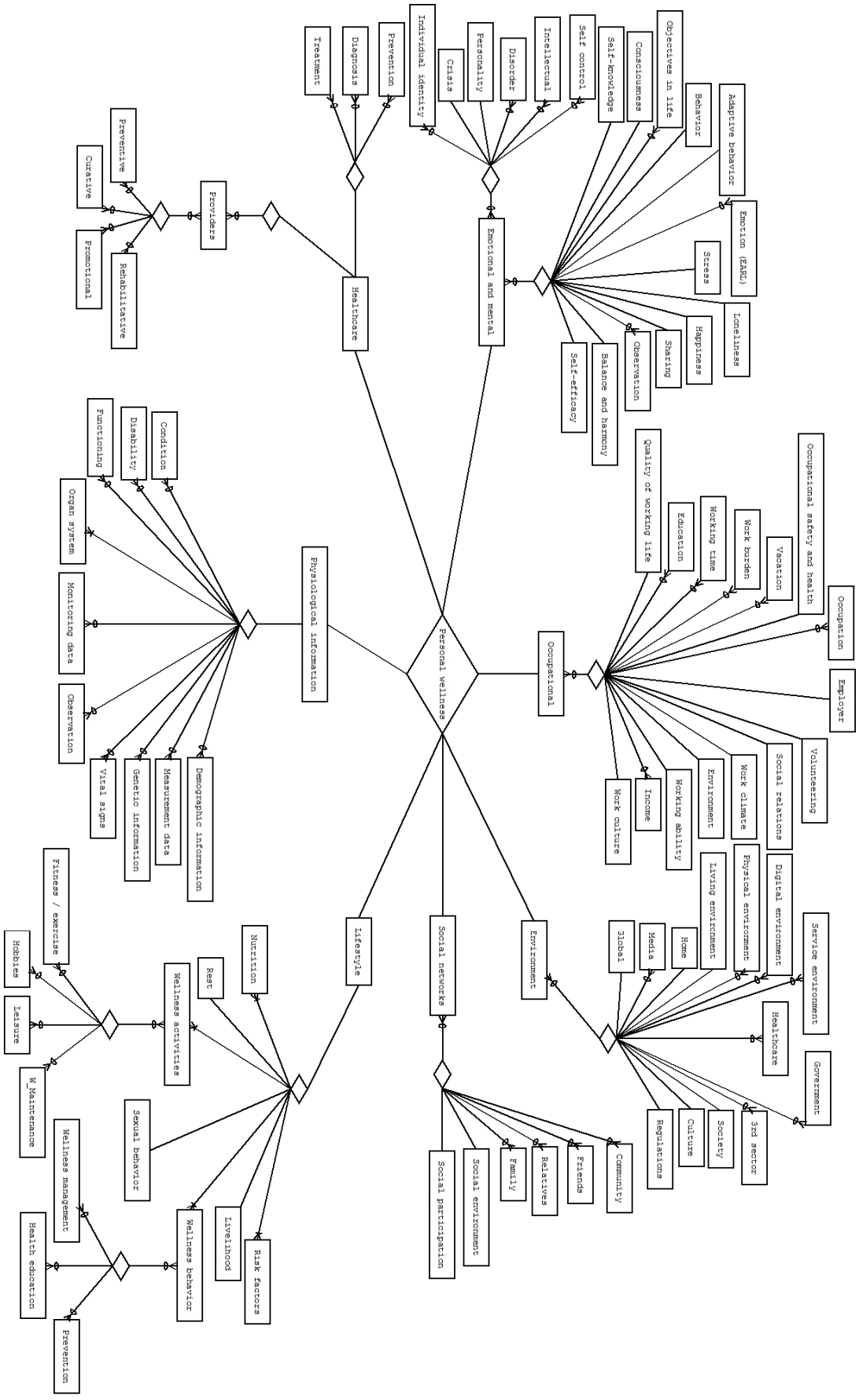


Figure 2. The highest level of the personal wellness information model.

The lifestyle component focuses on personal lifestyle and describes activities, behaviours and choices affecting daily life. Concepts in lifestyle are dependent on the person, who can usually affect, control, influence or manage these. The emphasis on concepts in lifestyle may vary widely between different people. The emotional and mental wellness component focuses on psychological issues such as emotions, identity and personality. It includes concepts that describe views, feelings, and attitudes toward life, experiences, possible disorders, and mental health. Emotional and mental wellness target the person's mind, how she will react to situations, and how she copes mentally.

Occupational wellness is about a person's occupation, which is a broader concept than work, as it covers being a student, unemployed, retired or other. The concepts in the component describe the actual occupation, its properties, its climate and how the person feels about it. Physiological wellness focuses on health and wellness related information outside the healthcare provider network. This component is designed to support citizens' activities in health and wellness management by allowing them to collect, observe and manage their personal information. Physiological wellness includes genetic information, vital signs, measuring and monitoring information collected, possibly with different devices and sensors, as well as information about a person's conditions and functioning as a whole.

The healthcare component focuses on regulated healthcare organisations and information in their health records. It is based on two main concepts: provider and service. Provider describes different healthcare organisations divided into four types: preventive, curative, promotional, and rehabilitative. Services are divided into three types: prevention, diagnosis, and treatment. All these create medical documents, hence composing a person's medical history. The social networks component describes a person's social relations, including family, friends, relatives, etc. It also contains different communities and social environments, and social participation in these contexts. The environment affects people in many ways, and it includes both digital and physical environments. The environment is heavily context-dependent, and it may vary widely between countries or even cities.

The personal wellness information model represents how citizens see their personal wellness, and what concepts, categories and relationships exist. These are the main components in ontology development.

5.3 Trustworthiness in pervasive health

Pervasive health is defined as a system which delivers health and wellness services in an open, unsecure and dynamic environment. Also, a set of principles are defined for the trusted processing of information in pervasive health (III). The concept of pervasive health has been initiated by new service models, a more complete view on health and wellness, personalised health and medicine and technological innovations. Pervasive health covers the concepts of ubiquitous or pervasive healthcare, but it is a broader concept as it supports services outside provider networks and fulfils the holistic view on health and wellness.

In this research, the definition of pervasive health has been extended from what has been presented earlier in the literature. Here, it has been defined as a meta-system – a system composed of systems (Figure 3.) (III). Pervasive health is an open and dynamic information space which utilises ubiquitous computing and consists of digital bubbles. A bubble offers services and contains information systems and their stakeholders. These bubbles can be linked together dynamically to create a network of health and wellness services. Bubbles, or systems, can collect, process, store and disclose personal health and wellness information.

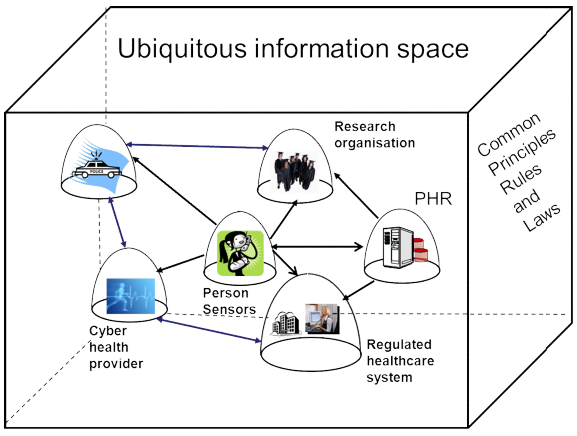


Figure 3. Pervasive health with interconnected systems.

In pervasive health, a person can create a personal health and wellness network and select, tailor and combine which services or systems participate. S/he can control information sharing between bubbles or their information systems. Although there are common principles and laws regulating information processing, there are

still differences between the bubbles' responsibilities and possibilities for information processing. For example, healthcare providers are heavily restricted by healthcare specific legislation and medical ethical codes compared to wellness service providers. Personal information is not necessarily stored in regulated EHRs, and this creates several issues concerning the privacy, security and trustworthiness of information.

The amount and variety of health and wellness related information is increasing, and it is also becoming more personal and private. Information can be any kind of personal information (e.g., behaviours, location, social activities, emotions, and rich contextual data) covering a person's entire life. Information processing in pervasive health can be autonomous, and it can happen even without the person in question knowing about it. Information content, processing and needed regulations differ widely from current processing, collecting and storing of healthcare information. The data content in pervasive health exceeds the contents of current EHRs. The use of personal information is not limited to health and wellness services, and it is of value to many different fields and businesses.

There are several stakeholders in pervasive health with different interests, objects, regulations and viewpoints. In paper III, the focus is on the interests and concerns of the person in question i.e., the data subject. To support the data subject's possibilities of ensuring trustworthiness in information processing in pervasive health, a set of principles for trusted pervasive health have been developed, namely, the THEWS-principles. The THEWS-principles specify that the data subject shall have the right to:

- Dynamically verify the trustworthiness of the pervasive health network s/he has created.
- Verify the trustworthiness of any system in the information space that requires or uses the data subject's personal health data for secondary purposes.
- Control the processing of personal health information, both inside systems and between them.
- Be aware of all events, situations, and contexts where the data subject's health data is collected, processed, stored, and disclosed.

- Define situation-specific, context-aware, and granular personal privacy and trust policies, which regulate how his or her health data is collected, processed, disclosed, shared, stored, or destroyed.

The THEWS-principles also state that systems and stakeholders have the responsibility to ensure:

- Trust verification by publishing their privacy policies, environmental, and contextual features.
- Openness of their interest, business needs, and policies as well as their relationships with other systems in the information space.
- Transparency of data processing.

The THEWS-principles emphasise the rights of citizens not only to be aware of the processing of their personal information, but also their right to control and limit the processing, collection, use and sharing of their information by setting own privileges and obligations (i.e., dynamic privacy and security policies). Persons should be able to verify in advance the trustworthiness of all participants. Trustworthiness in pervasive health means that the entire network of systems is trusted, data subjects' privacy has been protected, data is processed ethically, legally and that it follows the rules or policies defined by the data subject. The THEWS-principles offer protection against common threats of pervasive computing, facilitate trustworthiness, and support a person's information autonomy.

5.4 Feasibility of the privacy attributes of the personal wellness information model

The personal wellness model has been evaluated in a feasibility study (IV) to analyse whether it would result in a new understanding of personal wellness, its contents and limits and whether the defined privacy attributes (context, capability, competence, reliability, benefit, benevolence, and confidence) would be able to cover the needed aspects of privacy. As privacy is a highly personal and situation-dependent concept, it can usually only be analysed using qualitative means. Privacy metrics can be used to define good or bad privacy and how well applications or information systems fulfil privacy requirements. The defined privacy attributes are

partly based on empirical research conducted with focus groups and partly on a literature analysis.

The results show that in pervasive health, it is difficult for people to know the actual privacy status of the provider especially when considering non-regulated environments. This also creates trust related problems as the privacy and reliability of the information are out of a person's control. Transferring information from a regulated environment with proper security and privacy safeguards to a non-regulated environment can result in this information losing its reliability, and also, the original security and privacy policies may no longer be valid.

Notwithstanding, citizens should be aware of the privacy status of the services they use and be able to control their privacy whether they are in non-regulated or regulated environments. To achieve awareness, new privacy services have to be created to ensure processing and disclosure of information and to allow privacy services to monitor and measure the degree of privacy and the level of control over citizens' personal information. Importantly, these services should utilise trust-building measures. In personal wellness information, all concepts should have privacy attributes embedded in them which can be activated and made known, controllable and measurable. This requires a process-driven approach with predictive trust building, perceptions of the intentions of services, capability of evaluating providers and of supporting the transfer of information between regulated and non-regulated environments. Self-regulating policies are also needed to control and constrain processing in different contexts.

The feasibility study (IV) clearly shows that the wellness information model represents essential concepts and gives structure to the presentation, and it can be used to create instantiations. While the model describes a combination of regulated and non-regulated concepts, current privacy regulations do not support this kind of pervasive health environment. The defined privacy attributes help citizens to be aware of and control and measure the privacy of their personal information. New technological solutions are needed to implement these privacy attributes.

5.5 Trust information-based privacy architecture for ubiquitous health

Privacy in pervasive health is based on trust. Therefore, privacy architecture for pervasive health must be based on trust information. The features of privacy architecture should consider the nature of pervasive health, trust and privacy aspects of systems offering services, regulatory requirements and persons' privacy needs. The architecture should try to solve persons' concerns on:

1. How trustworthy the system is?
2. How to improve the lack of awareness and transparency in data collection and processing?
3. Who is using the data inside a system?
4. How to guarantee that data is processed lawfully?
5. How to guarantee that data is processed according to person's personal policies?

Layered architecture framework model (VI) is based on three layers (Figure 4.). The top layer describes the common services for all stakeholders. The middle layer describes needed privacy and trust services. The bottom layer is the network layer where all participating entities are located. In Figure 4. the DS means the data subject, PHI is personal health information, S is a system and D means domain. The privacy architecture is developed to manage information privacy using services and by supporting context-aware privacy policies using trust information. The architecture combine several privacy and trust approaches including trust calculation, policies, context services and monitoring services.

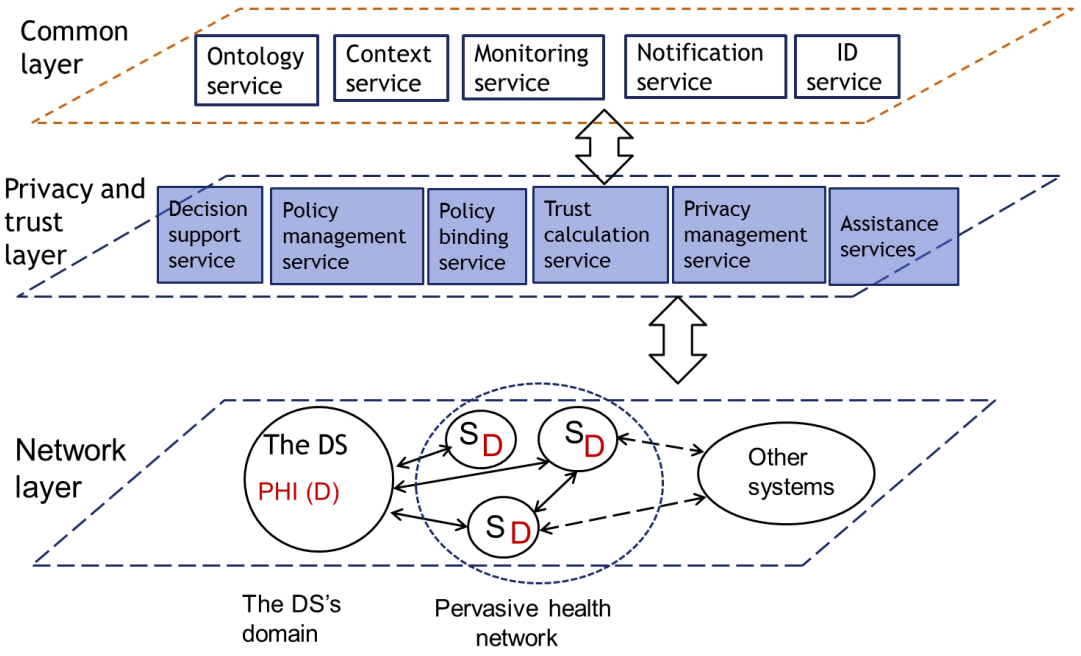


Figure 4. The framework model for the privacy architecture

As it is practically impossible for persons' to be able to evaluate trustworthiness of systems the trust calculator is included in the architecture. Trust calculator is not a decision maker. It calculates the trust information of a system by using the published information, available contextual data, system's measured or monitored features and system's past history. It also offers assistance services for persons' to interpret the trust information and help them with policies. With trust information persons can predict system's willingness or ability to process information according to personal policies or regulations. Trust calculator also informs how trustworthy a system is, what kind of policies and technical architecture a system has and how system's policies comply with regulations and legislation.

The context service captures context information of all participating entities and makes it available to trust calculator and to persons using ontologies. Monitoring service gives feedback, reduces risks and detects conflicts with personal policies and possible information processing. Notification service is used to communicate between a person and a system and to improve transparency by expressing personal policies to systems and to publish systems policies and relations to other systems. In this architecture the person is the final decision maker concerning the rules he/she

wants to include in the system specific privacy policy. Decision support service and policy binding service are tools to help the person in this process.

The privacy management architecture is designed to fulfil the principles for trusted information processing (III) and also it offers protection against many known privacy threats of ubiquitous computing.

5.6 Context-aware privacy for pervasive health

In pervasive health, services can be regulated healthcare services or other services depending on the status of the system. There are also general regulations concerning privacy and security and other domain specific regulations which can limit and constrain participants and their actions. Systems and persons have to discuss trust and privacy levels to enable access to personal information in exchange for needed services. The higher the level of trust a person has in a system, the lower the amount of needed privacy policies to protect information. To implement privacy policies privacy attributes are needed. One of the key privacy attributes is context which refers to the situation where the data and information are created or processed. In paper VI pervasive health is further developed by analysing privacy attribute context and its contents.

Privacy related context information makes it possible to create context-aware privacy policies which can adapt to situation changes. It can also be used in trust negotiations between participants by comparing person's privacy policies and original context of information into possible use context. As systems, services and information processing vary, the original context of the information as well as its use context have to be captured. In many cases, original and use contexts of information differ widely, and it is critical to differentiate these two. Different contexts have different requirements and constraints for information processing.

To identify privacy related context information typical activities of pervasive health have been analysed with scenarios. The privacy related context information of pervasive health seeks to identify the following:

- What happens?
- Who is the target or actor?

- What services are related to the situation?
- In what kind of environment(s) does this situation happen?
- Who are the actors and interested stakeholders?
- What information systems participate in the situation?

Thus, the main components for privacy related context information are concluded as: situation, person, service, environment, stakeholder and IT system. These components enable situations to be captured in multidimensional and multidisciplinary environments. By combining the results of the user scenario analyses and the research on the principles of trusted information processing (III), defined privacy attributes (IV) and the required information for privacy policies (V) more detailed attributes are derived for the components (Figure 5).

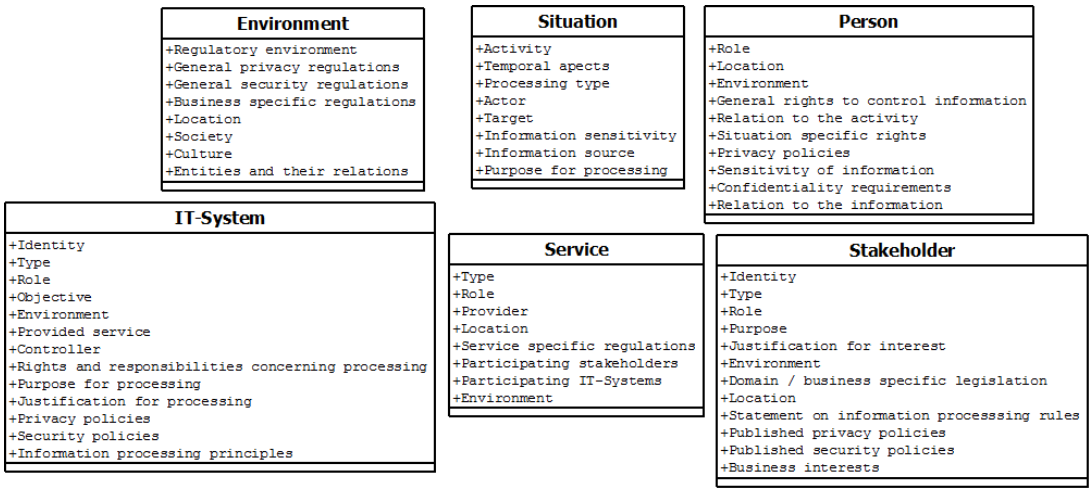


Figure 5. Privacy related context information of pervasive health.

The situation is the core component because of the dynamic nature of pervasive health and the limitations in predefining actions and entities. Situations describe information processing that happens in a certain context because of some activity and by/for a certain person. Situations can be created by a person, a service, a stakeholder or an IT system. Pervasive health environments can vary widely between situations (e.g., regulations, entities, culture), and they can be either digital or physical. Environments may have different properties for privacy, security and trust, hence the environment of a situation and all participating entities, including their own environment, have to be captured.

The person component can create, be part of and/or be the target of a situation. The service component describes different health and wellness related services. Services can be provided by different IT systems or stakeholders and can be regulated by some regulations or legislation (e.g., healthcare specific, privacy or security related, domain specific). The IT system component describes computational entities linked to pervasive health (e.g., EHR, PHR, PHS, pervasive systems, wellness management systems, monitoring and measuring devices, and sensors). Stakeholders represent social actors or interested parties that offer, participate or are interested in a situation.

The resulting components and their attributes describe what privacy related context information is needed in pervasive health to increase trustworthiness in information processing. A situation's parameters may vary widely; hence general components are needed to capture context information. The components and their attributes enable the capturing of high-level definitions of situations happening in the pervasive health environment and domain specific information, such as information about characteristics of an environment. These components can be used to create context-aware privacy policies and to analyse that the information processing follows the person's personal privacy preferences and the requirements from the original context of the information.

5.7 Summary of the results

In this dissertation, I have combined a citizen-centred health paradigm with new technological innovations, such as pervasive computing, and have created a vision for future healthcare. I have presented how to enable a distributed, personalised and holistic view on health and wellness to satisfy the need for collaboration throughout the care processes. I have also produced an information model of personal wellness that supports progress towards more complete health and wellness care. The information model defines the information basis for complete health and wellness management. It can be used as a starting point to create a personal wellness ontology which enables semantic interoperability between different actors and the creation of distributed health and wellness services.

In this dissertation pervasive health is defined as a meta-system, a system about systems. In pervasive health, services are produced in collaboration and can be offered by different providers and information systems. Citizens can select, tailor and combine different services and systems. The vision of pervasive health enables true personalisation and consumerism in healthcare delivery. It enables a citizen-centred healthcare paradigm by combining regulated and non-regulated services, as well as providers, based on personal preferences.

The key issues hindering widespread implementation of pervasive computing are privacy and trustworthiness, and in this dissertation, I have further developed the idea of pervasive reality by analysing pervasive health in the context of privacy and trustworthiness. I have defined a set of principles for making pervasive health trustworthy, namely, the THEWS-principles, which give citizens the right to control their personal information and its processing and disclosure. These principles can also be widened to cover all pervasive computing. Novel privacy management architecture is presented which is based on trust information. The architecture is designed to ensure and manage privacy of personal information. I have also presented the idea of using privacy related context information for privacy protection in ubiquitous health.

In summary, I have presented a vision of how healthcare should be organised and offered, the information basis for more complete and holistic health and the kind of HIT systems needed. In this thesis, new rights for citizens and responsibilities for information processing organisations have been defined to describe how information processing can be made trustworthy, thereby honouring citizens' privacy. An important result of this dissertation is a vision for a new kind of trust information based privacy management architecture which utilises privacy related context information.

6. Discussion

6.1 Discussion

The purpose of this dissertation is to produce basic knowledge with artefacts at two levels: constructs and models. These artefacts support the progress of pervasive health. The results also outline the needed methods and instantiations that enable the creation of concrete artefacts in the future. This dissertation provides results in the fields of health informatics, pervasive computing and privacy management. The five main objectives of this dissertation are:

1. To analyse the citizen-centred healthcare paradigm in the literature and to create a vision for future healthcare.
2. To create a high-level personal wellness information model describing how people conceptualise their personal wellness.
3. To define pervasive health as a system, analyse its privacy and trust challenges and define the principles for making it trustworthy.
4. To develop a privacy management architecture to help citizens to control their privacy and information processing in pervasive health.
5. To analyse what kind of context information is needed to enable trust in information processing and to enable citizens' rights to privacy.

To fulfil these objectives, this dissertation:

1. Presents a vision for future collaborative healthcare to realise the citizen-centred care paradigm.
2. Introduces a personal wellness information model that captures the main concepts of a holistic view on health and wellness.
3. Suggests principles which guarantee the trustworthiness of information processing in pervasive health.
4. Presents a novel privacy management architecture based on trust information.

5. Describes the required privacy related context information components to ensure citizens' rights to privacy and to enable adaptable privacy services.

Health information is currently fragmented into different organisations and information systems, and therefore, it is almost impossible to have a clear picture of a person's complete health and wellness (3; 13; 55). For the future of healthcare, it is crucial that citizen's personal health information is collected in a cross-organisational and lifelong way and is accessible to all relevant participants throughout the care process to enable collaboration and distributed care services. Preventive services and early diagnostics require knowledge of an individual's normal functions (156). Also, many initiatives on better lifestyles and chronic disease management occur outside healthcare organisations and their information systems. Collaborative information systems are needed for the seamless sharing of information. There are tools (e.g., PHR) which could be used to improve collaboration between citizens and professionals and to enable continuous care processes. The current challenge is that there is no real interoperability between health information systems and the information systems designed to support citizens' actions towards healthier lifestyles (4; 55; 90).

In the future of healthcare, the importance of citizens' role in their care will increase and citizens have to be seen as important actors (12; 13; 53; 94). This dissertation realises that by presenting a vision for a new collaborative healthcare (I), citizens can control their own health and wellness information and create and tailor their own service networks as distributed and collaborative. This vision enables information sharing among participants and includes services that are also provided by non-regulated health and wellness providers. The regulative liabilities of licensed healthcare providers (e.g., care documentation, licensed professionals) do not change.

The knowledge basis for supporting a more complete and holistic view on health and wellness, which incorporates citizens' perspectives, has not been widely researched (157). Without understanding the knowledge behind the phenomenon, and capturing the concepts and their meanings and relationships, it is almost impossible to create real interoperability in the domain (158). To support the efforts for semantic interoperability, the personal wellness information model has been developed to describe the domain of complete health and wellness from citizens'

perspective (II). As most of the models or ontologies in previous research are created for regulated healthcare, and the concept of wellness focuses on assessing or measuring wellness, this model brings new knowledge to the field of health informatics. The information model defines the scope and contents of personal wellness based on the literature and empirical research. The model captures and represents the views of active and conscious people who are not medical professionals.

The information model (II) defines more than 200 concepts and their meanings. Personal wellness and its scope have been outlined using these concepts and their basic relationships. The model captures the main components of personal wellness, the information and contexts related to it and its influences. Although it is quite a high-level model, it can be used as a basis for ontology development. Notwithstanding, there are limitations in the model, for example, some of the concepts are quite abstract and explicitly defining them can be challenging. Nonetheless, this model is a good starting point for more detailed research concerning personal health and wellness and how the knowledge basis for semantic interoperability can be constructed. Pinto and Martins (33) see conceptual models as a crucial stage in ontology building as these models can be used to conceptualise the domain of discourse. Conceptual models represent, either at an informal or semi-formal level, the concepts and their relationships in the domain. This research has started the development of an ontology of personal wellness by presenting and structuring the domain.

To further advance healthcare as more personalised, citizen-centred and HIT-enhanced, an extended definition of pervasive health has been presented (III). This definition identifies pervasive health as a system composed of linked bubbles, i.e. digital territories consisting of information systems, their stakeholders and environments. All bubbles have their own processing regulations, rules and principles based on their characteristics. In pervasive health, services can be offered anywhere and anytime, and it truly realises the citizen-centred healthcare paradigm as it allows citizens to control and tailor the services they use and even control how their personal information is, or can be, used. Citizens and providers have to negotiate the terms of service provision, and in exchange for services citizens have to share their personal information with providers. Hence, citizens have to be able to calculate or estimate the trustworthiness of the service provider, and based on that,

negotiate how personal information is, and can be, used. The higher citizens' trust is, the lower the need for privacy protection and vice versa.

Privacy is probably the most significant issue hindering widespread usage of pervasive technologies (143). Most information about people and their personal communication can be captured and processed, and different monitoring and autonomous computing entities may create a feeling of continuous surveillance. To reduce fears concerning pervasive technologies, citizens have to be able to control their privacy. In Ruotsalainen et al. (159), we have analysed the key privacy and security threats of pervasive health as:

- A digital footprint is created from every event,
- Context information can easily be misused,
- Security characteristics of information can change because of linking heterogeneous information together,
- Navigation without context-dependent authorisation may cause privacy breaches,
- Monitoring of an individual's activities and behaviour is possible,
- Data can be collected without an individual's knowledge,
- Limited possibilities to control secondary use, and
- The information space has unlimited memory.

The feasibility analysis (IV) shows that in pervasive health, it is challenging for citizens to control their privacy and trust in non-regulated environments. Based on the feasibility analysis, it is obvious that new technological solutions are needed to enable citizens to control their privacy and to calculate the trustworthiness of systems.

To enable trust in the processing of personal information in pervasive health, the THEWS-principles have been defined (III). In these principles, the basic assumption of privacy management has shifted from traditional static protection and risk-based thinking with predefined security policies into a more dynamic control of privacy and trust. This shift presents a new perspective for privacy management, a necessity in open information spaces. The key points in the THEWS-principles are to guarantee citizens' right to privacy, to ensure citizens' awareness of information processing and their ability to control their information and its processing. The THEWS-principles emphasise the importance of transferring the control of privacy

to the data subject, and to make it as his/her basic right in information processing. These rights can be fulfilled with personal privacy and security policies which can ensure that information systems process data only according to the personal preferences of the citizen. Policies should be dynamic and capable of adapting to changing contexts. As Schaub et al. (141) point out, privacy solutions should, in pervasive environments, be able to perceive context information and to adapt according to it.

Privacy cannot be guaranteed in pervasive environments with traditional security means; instead, privacy should be based on trust and its properties (98; 133; 134). In paper V a novel architecture for privacy management in pervasive health is presented. This architecture increases transparency of information processing and gives citizens tools to manage their privacy and to control how their personal information is, and can be, used. The privacy architecture helps citizens to manage their privacy dynamically and to create context-aware privacy policies. It also assists in trust negotiations and in evaluating system trustworthiness. The presented architecture illustrates how the THEWS-principles defined in this dissertation can be realised. The architecture is based on trust information and is capable of making automatic and autonomous decisions based on measured values, monitored functioning of the systems and personal policies, thus, exceeding the capabilities of traditional security services based on access control. The privacy architecture is dynamic, context-aware and platform-independent, meaning that it can be implemented with different technologies.

This dissertation presents an approach how privacy related context information can be used in privacy management in pervasive health (VI). The privacy related context of information processing can be used as part of personal privacy policies. Policies also enable citizens to define the kinds of use contexts in which their information can be processed. By comparing privacy policies, original and use contexts, privacy architecture can make automatic decisions that honour personal preferences. In pervasive health, information can be processed in many environments and contexts, and therefore, it is crucial to differentiate these two contexts and to be able to create context-aware privacy policies. My view is that by using context information components to build privacy, one can ensure trusted processing with policies and services which are dynamically capable of adapting to changing contexts. Citizens should be able to control the kinds of contexts in which

their personal information can be processed. Context information can also be used in trust negotiations when deciding whether information disclosure or processing is allowed, or whether extra security measures are needed (e.g., partial disclosure, anonymisation, and encryption). The components presented (VI) can be used to capture privacy aspects of information processing.

This research has utilised healthcare as a domain, however, the results presented in this dissertation can easily be generalised to contribute to the whole pervasive computing field by introducing this new privacy architecture and privacy related context information components. This kind of solution has not yet been presented in the literature, although it has been acknowledged that privacy services should be able to adapt to different contexts.

The vision described in this dissertation is, to some extent, already a reality. The technology mostly exists, but it still lacks the capability to integrate all these technologies, processes, information and actors to create a seamless network of services, and at the same time, still honouring citizens' privacy. This dissertation further develops the vision of pervasive health by defining the information basis, the system required and how to enable trust in information processing. There are still several challenges hindering the full implementation of pervasive health. Citizens need new tools to help them manage their information and privacy, control information processing and support decisions concerning the trustworthiness of participating systems. Also, creating privacy policies should be as easy as possible and at a very high level, that it would not require special skills. Privacy services should be automatic, autonomous, context-aware, dynamic and capable of learning from the choices and behaviours of citizen and service providers.

Despite the technological challenges, the main issues hindering pervasive health are arguably political and organisational. The political challenge is to enforce the THEWS-principles as companies, governments or healthcare organisations may inhibit their implementation. Implementing the THEWS-principles means changes to legislation as well as to organisations' processes. The key issues for trusted information processing are the openness and transparency of information processors. They should be obliged to publish their privacy and security policies and their principles for information processing. With this published information, citizens could then evaluate service providers' trustworthiness. Citizens should be able to

control, monitor and evaluate the processing of their personal information even inside systems.

Current legislation does not support this kind of privacy management. Healthcare organisations and professionals may not be ready for the transformation to a citizen-centred model and to share control and power with citizens. Change is required in attitudes and in a willingness to support citizens' participation and possibilities to manage their own health and wellness. Citizens have to be seen as active and important participants and they need rights and possibilities to participate. Also, it remains questionable whether citizens are ready, willing and capable of managing their own health and wellness.

6.2 Reliability and validity

In qualitative research, reliability and validity are conceptualised as trustworthiness, rigor and quality (160). According to Whittemore et al. (161), qualitative research is based on creativity, but it should not limit the quality of the science, and it should be balanced with reasonable claims, evidence and critical use of methods. In qualitative research, some validity criteria, methodological procedures and guidelines are essential to ensure the scientific quality of the research (161; 162). In qualitative research, the role of the researcher influences the reliability and validity of the results. To improve quality, this research has been conducted with an open mind, critically assessing materials and produced artefacts (163).

This dissertation has utilised design science (DS) research as its scientific framework as well as different methods applied under it. The DS research methodology, along with the build-evaluate approach, has been followed by complying with the seven guidelines for performing DS research (21). These guidelines have provided the validity criteria with which to analyse reliability and validity. Following these guidelines, the importance of this research has been evaluated as highly relevant since healthcare appears to be in a transitional phase, and privacy and trust are the key issues in pervasive computing. Actual artefacts have been built in the form of constructs and models, and the results contribute to the fields of pervasive computing and health informatics. Design processes have been performed iteratively and as a search process for a solution.

Considering the DS guidelines (21), the most important issue with reliability and validity is that the evaluation and assessment of the results are limited, although a feasibility study has been performed, and evaluation has been a feature of the focus groups. As this dissertation focuses on constructs and models, further research is needed on methods and instantiations to be able to evaluate the produced artefacts in practise. The guidelines (21) emphasise that researchers should use rigorous methods, and this has been approached by having several focus groups with different backgrounds and age groups and by creating several types of scenarios to capture a wide scope of views and aspects.

The research presented in this dissertation has followed the International Medical Informatics Association's (IMIA) code of ethics for health information professionals (164) and its ethical principles for conducting research. The empirical research has been executed on a voluntary basis and the objective has been to capture participants' opinions and views. Information regarding participants' health or wellness or other personal information was not collected. Moreover, opinions and views have been anonymised. The purpose and objectives of the research and the use of collected information was explained to participants prior to the focus group interviews.

This research has emphasised citizens' viewpoint instead of those of medical professionals. As the research domain is complex and quite abstract, a qualitative research approach has been adopted. The domain of personal wellness is very wide and complex with many variables, and the amount of existing knowledge has been limited. In these kinds of situations, focus groups are seen as a very suitable method (24; 25).

There was a total of six focus group meetings with four separate groups, and the author was in charge of these meetings. The emphasis was on the discussion within the groups and the author only guided the meetings with themes and results from previous meetings. The focus groups were purposely small (4-10 participants) in order to ensure that all participants were able to express their opinions and views. Although focus groups were suitable for this research, some limitations were recorded. As participants were selected from limited pools of potential participants, and on a voluntary basis, they may have been a bit more active and conscious of their health and wellness than the average citizen. Also, participants were all

Finnish, and wellness is usually seen as a very context-dependent concept. As such, the resulting information model described a Finnish view on the matter, although the literature was mostly international.

The focus group meetings were recorded, following which, the material was transcribed and the results were represented in the information model. Modelling was performed iteratively and the resulting model was evaluated with the focus groups. Modelling was done with a simplified entity relationship (ER) notation so that the models could be understood and modified by participants without actual modelling experience. The actual modelling was performed by the researcher. In the information model, there are some limitations as some of the concepts are quite abstract and defining them explicitly in an ontology can be challenging. As the domain is very complex, there might be additional views than what are included in this dissertation.

As pervasive health is still a view of the future, use scenarios and user stories were used to predict future use and systems. The problem with these scenarios is that they represent a subjective view on the future, based on an idea of pervasive health. This view is heuristic by nature and mostly based on existing literature and knowledge that I have processed and filtered. As this research is based on a predicted and subjective future, the results may not be true in all possible futures and the components represent just one view on needed context information. They may not be conclusive, complete or final. Also, the whole paradigm of citizen-centred care with innovative technologies is still one possible future, although it is widely predicted to be the future healthcare paradigm.

6.3 Directions for future research

This dissertation has presented a new vision of healthcare, analysed its privacy threats, risks and requirements and presented a new way of managing privacy in pervasive environments. Based on the results of this dissertation, three main themes for future research have been identified:

- Personal health and wellness ontology,

- Development of ontologies for context information, trust, privacy and policies,
- Requirements for new legislation to support citizens' rights to privacy in pervasive environments.

To create semantic interoperability in the pervasive health ecosystem, and to enable seamless networks of services, further research is needed. The personal wellness information model has defined over 200 concepts and the model can be used as a basis for a high-level personal wellness ontology. This ontology would define the main concepts and their relationships in a formalised, computer understandable format and could act as a vocabulary for all systems participating in pervasive health. The personal wellness ontology could be used to integrate different domain ontologies to enable semantic interoperability and shared understanding of all different concepts.

In this dissertation, context information components for pervasive health have been defined but they require further research. Context and trust information is widely dependent on the information published by organisations. Further analysis is needed to understand what information is necessary for evaluating and calculating the trustworthiness of different stakeholders. Research is also needed to define what sorts of security and privacy policies and trust information organisations should publish and in what format they should be released.

To create context-aware privacy services in practise, several ontologies are needed. These ontologies should represent, in a formal way, all necessary activities, services, IT systems, stakeholders, information content and legislative environment. Also, the concepts related to trust, privacy, security and policies have to be modelled in ontologies. The use of ontologies enables semantic interoperability and the creation of computational rules and constraints fulfilling the requirements, constraints, responsibilities and rights set by legislation and personal policies. Also, authorities or certified organisations, that can audit and control information processing in organisations need new rights and knowledge for measuring the trustworthiness of information processors.

The third future research theme arising from the results is the analysis of requirements for new legislation. Detailed research and public discussion are needed to analyse the challenges set by the healthcare transition and how pervasive

environments affect processing of personal information, privacy and citizens' rights and possibilities to control their personal information. Also, research and public debate are needed to decide what kinds of requirements, constraints and responsibilities should be set for organisations willing to process personal information.

7. Conclusions

The purpose of this dissertation was to produce additional knowledge on pervasive health in order to advance citizen-centred healthcare. The objectives were to define a vision for future healthcare, to create an information model describing how people conceptualised their personal wellness, to analyse privacy threats of pervasive health, to develop privacy management architecture and define privacy related context information which is needed to enable trust in pervasive health.

This dissertation therefore presents five major contributions:

1. A vision for future collaborative healthcare which advances the citizen-centred care paradigm.
2. A high-level personal wellness information model describing the conceptualisation of how people see their own personal wellness.
3. A set of principles which can be used to enable trust in pervasive health. These principles shift privacy management from traditional, static risk-based thinking to a more dynamic and trust-based approach.
4. A privacy management architecture based on trust information to ensure and manage privacy of personal health and wellness information.
5. Privacy related context information components which can be used to define privacy policies and capture information processing contexts in pervasive health, thus enabling context-based privacy management.

This dissertation extends new knowledge to the fields of health informatics, pervasive computing and privacy management by presenting artefacts – constructs and models. It presents a new way of using situational information as a basis for privacy management. The research has some limitations. The empirical research focused on Finnish people, and therefore, the views presented in the information model are from a Finnish perspective. However, the literature studied has been broadly international in scope. Qualitative research is usually heavily dependent on the researcher and his/her specific skills, a dynamic encountered in this dissertation. The scenarios are based on a predicted future and on the knowledge of the author,

and therefore, the results based on the scenarios presented may have some limitations.

References

[1] Codagnone C. Reconstructing the whole: Present and future of personal health systems. European Commission, 2009, http://www.evia.imasdtic.es/cli_aetic/ftpportalweb/documentos/phs2020-book-rev16082009.pdf. Accessed 17 May 2013.

[2] PricewaterhouseCoopers Health Research Institute. Healthcast 2020: Creating a sustainable future. PricewaterhouseCoopers, http://www.pwc.com/en_GX/gx/healthcare/healthcast-series-future-trends/assets/pwc-healthcast-2020-creating-a-sustainable-future.pdf. Accessed 28 May 2013.

[3] Varshney U. Pervasive healthcare and wireless health monitoring. Mobile Networks and Applications. 2007;12:113-127.

[4] Wartena F, Muskens J and Schmitt L. Continua: The impact of a personal telehealth ecosystem. eHealth, Telemedicine, and Social Medicine (eTELEMED '09), 1-7 Feb. 2009, p 13-18.

[5] Teperi J, Porter ME, Vuorenkoski L and Baron J. The Finnish health care system: A value-based perspective. Sitra Reports 82, 2009 http://www.sitra.fi Accessed 17 May 2013.

[6] Atallah L, Lo B and Yang GZ. Can pervasive sensing address current challenges in global healthcare? Journal of Epidemiology and Global Health. 2012;2:1-13.

[7] Ludwick DA and Doucette J. Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries. Int J Med Inform. 2009 Jan; 78(1):22-31.

[8] Haux R. Health information systems - past, present, future. Int J Med Inform. 2006 Mar-Apr;75(3-4):268-81.

[9] Monteagudo JL and Moreno O. D2.5, Report on Priority Topic Cluster two: Patient Empowerment. eHealth ERA, 2007 (http://www.ehealth-era.org/documents/eH-ERA_D2.5_Patient_Empowerment_Final_31-03-2007_revised.pdf). Accessed 17 May 2013.

[10] Detmer D and Steen E. Learning from abroad: Lessons and questions on personal health records for national policy. The American Association of Retired Persons (AARP), 2006, http://assets.aarp.org/rgcenter/health/2006_10_phr_abroad.pdf . Accessed 17 May 2013.

[11] Rigby M. Integrating Health and Social Care Informatics to Enable Holistic Health Care. Stud Health Technol Inform. 2012;177:41-51.

[12] Downing GJ. Key aspects of health system change on the path to personalized medicine. Transl Res. 2009 Dec; 154(6):272-6.

[13] Pratt W, Unruh K, Civan A and Skeels M. Personal health information management. Communication of the ACM. 2006;49(1):51–5.

[14] Ohashi M, Hori M and Suzuki S. Citizen-centric e-healthcare management based on pervasive authentication – New ICT roadmap to active ageing. Pervasive Computing Technologies for Healthcare (PervasiveHealth), 22-25 March 2010, p 1-8.

[15] Nykänen P. Requirements for user friendly personal ehealth information systems. Stud Health Technol Inform. 2008;137:367–372.

[16] Koop CE, Mosher R, Kun L, Geiling J, Grigg E, Long S, Macedonia C, Merrell R, Satava R and Rosen J. Future delivery of health care: Cybercare. IEEE Engineering in Medicine and Biology Magazine. 2008 Nov-Dec;27(6):29–38.
[17] Korhonen I and Bardram JE. Introduction to the special section on pervasive healthcare. IEEE Transactions on Information Technology in Biomedicine. 2004;8(3):229–234.
[18] Bardram JE. Pervasive healthcare as a scientific discipline. Methods Inf Med. 2008;47(3):178-185.
[19] Arnrich B, Mayora O, Bardram J and Tröster G. Pervasive healthcare: Paving the way for a pervasive, user-centered and preventive healthcare model. Methods Inf Med 2010;49(1):67-73.
[20] March ST and Smith GF. Design and natural science research on information technology. Decision Support Systems. 1995;15(4):251-266.
[21] Hevner AR, March ST, Park J and Ram S. Design science in information systems research. MIS Quarterly. 2004:28(1):75-105.
[22] Alturki A, Gable GG and Bandara W. A design science research roadmap. Lecture Notes in Computer Science. 2011;6629:107-123.
[23] Indulska M and Recke JC. Design science in IS research: a literature analysis. In: Gregor S and Ho S (Eds.), 4th Biennial ANU Workshop on Information Systems Foundations, 2-3 October 2008:285-303, Canberra, Australia.
[24] Kitzinger J. Introducing focus groups. BMJ. 1995;311(7000):299–303.
[25] Powell RA and Single HM. Focus groups. International Journal for Quality in Health Care. 1996;8(5):499-504.
[26] Mylopoulos J. Information Modeling in the Time of the Revolution. Information Systems. 1998 Jun;23(3-4):127-155.
[27] Siau K and Wang Y. Cognitive evaluation of information modeling methods. Information and Software Technology. 2007;49(5):455-474.
[28] Wand Y, Monarchi DE, Parsons J and Woo CC. Theoretical foundations for conceptual modelling in information systems development. Decision Support Systems. 1995;15(4):285-304.
[29] Weber R. Conceptual modelling and ontology: possibilities and pitfalls. Journal of Database Management. 2003;14(3):1-20.
[30] Mylopoulos J. Conceptual modeling and telos. In: P. Loucopoulos and R. Zicari (Eds), Conceptual modeling, databases, and CASE. Wiley, 1992:49-68.
[31] Wand Y and Weber R. Research Commentary: Information Systems and Conceptual Modeling - A Research Agenda. Information Systems Research. 2002 Dec;13(4):363-376.
[32] Johnson J and Henderson A. Conceptual models: begin by designing what to design. Interactions. 2002 Jan; 9(1):25-32.
[33] Pinto HS and Martins JP. Ontologies: how can they be built?. Knowledge and Information Systems. 2004;6(4):441–464.
[34] Institute of Electrical and Electronics Engineers (IEEE) Computer Society. IEEE Standard 1471-2000: Recommended Practice for Architectural Description of Software-Intensive Systems. Piscataway, NJ: IEEE; 2000.
[35] Carroll JM. Five reasons for scenario-based design. Interacting with Computers. 2000;13:43-60.
[36] Rolland C, Achour CB, Cauvet C, Ralyte J, Sutcliffe A, Maiden N, et al. A proposal for a scenario classification framework. Requirements Engineering. 1998;3(1):23-47.
[37] Arain M, Campbell MJ, Cooper CL and Lancaster GA. What is a pilot or feasibility study? A review of current practice and editorial policy. BMC Med Res Methodol. 2010;10:67.
[38] Belanger F and Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly. 2011:35(4):1017–1041.

[39] Lederer S, Deay AK and Mankoff J. A conceptual model and metaphor of everyday privacy in ubiquitous computing environments. UC Berkeley College of Engineering Technical Reports. Berkeley, CA: Computer Science Division, University of California; 2002 Jun. URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2002/CSD-02-1188.pdf, Accessed 4 Jun 2013.
[40] Skinner G, Song Han and Chang E. Defining and Protecting Meta Privacy: A New Conceptual Framework Within Information Privacy. Proceedings. 22nd International Conference on Data Engineering Workshops, 2006:101-107.
[41] Saltzer JH and Schroeder MD. The Protection of Information in Computer Systems. Proceedings of the IEEE. 1975;63(9):1278-1308.
[42] Westin AF. Social and political dimensions of privacy. Journal of Social Issues. 2003 Jul;59(2):431-453.
[43] Smith JH, Dinev T and Xu H. Information Privacy Research – An Interdisciplinary Review. MIS Quarterly. 2011;35(4):989-1016.
[44] Clarke R. Internet Privacy Concerns Confirm the Case for Intervention. Communications of the ACM. 1999;42(2):60-67.
[45] Pavlou PA. State of the information privacy literature: where are we now and where should we go? MIS Quarterly. 2011;35(4):977–988.
[46] Schoorman FD, Mayer R and Davis J. An Interactive Model of Organisational trust: Past, Present and Future. Academy of Management Review. 2007;32(2):344-354.
[47] Abdul-Rahman A and Hailes S (2000). Supporting Trust in Virtual Communities. Proceedings of the 33rd Hawaii International Conference on System Sciences; Jan 4-7, 2000; IEEE Computer Society, Washington, DC, USA.
[48] Gambetta D. Can we trust. In Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, Department of Sociology, University of Oxford, Basil Blackwell, Oxford, 1990, pp. 213-237.
[49] Abdul-Rahman A, Hailes S. A Distributed Trust Model. In: Proceedings of the 1997 workshop on New security paradigms, 48 – 60, ACM New York, NY, USA 1997.
[50] Larson JS. The conceptualization of health. Medical Care Research and Review. 1999;56(2):123-136.
[51] Tang PC and Lansky D. The missing link: Bridging the patient — Provider health information gap. Health Affairs. 2005 Sep/Oct;24(5):1290-1295.
[52] Continua Health Alliance. Connected Personal Health in 2015: "Getting it Right!" - Looking back on the emergence of integrated person-centered health. Continua Health Alliance, http://www.continuaalliance.org/sites/default/files/CHA_WP081408v07.pdf Accessed 17 May 2013.
[53] Kolitsi Z and Cabrera MF. Personal health systems: Deployment opportunities and ICT research challenges – Conference report . February 12–13, 2007, Brussels. European Commission http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=323 . Accessed 17 May 2013.
[54] Berry LL and Mirabito AM. Innovative healthcare delivery. Business Horizons. 2010;53:157-169.
[55] Bates DW and Bitton A. The future of health information technology in the patient-centered medical home. Health Aff (Millwood). 2010 Apr; 29(4):614-21.
[56] De la Fuente MW and Ros L. A health collaborative network focus on self care processes in a personal assistant. IFIP Advances in ICT. 2009; 307:759-766.
[57] Boulos MNK and Wheeler S. The emerging Web 2.0 Social software: An enabling suite of sociable technologies in health and health care education. Health Information and Libraries Journal. 2007;24(1):2–23.

[58] Kaplan AM and Haenlein M. Users of the world, unite! The challenges and opportunities of social media. Business Horizons. 2010;53:59–68.
[59] Hawn, C. Report from the field: Take two aspirins and tweet me in the morning: How twitter, facebook and other social media are reshaping health care. Health Affairs. 2009;28(2):361-368.
[60] Halonen, R. Social media as a means of peer support. In: Suomi R and Ilveskoski I (Eds.), Navigating the fragmented innovation landscape. Proceedings of the 3rd international conference on well-being in the information society (WIS2010). TUCS General Publication 56, August, Turku, Finland, 2010:48–60.
[61] World Health Organization. Gaining health – The European strategy for the prevention and control of noncommunicable diseases. WHO, Regional Office for Europe Copenhagen, Denmark, 2006.
[62] Mattila E, Korhonen I, Salminen JH, Ahtinen A, Koskinen E, Sarela A, Parkka J and Lappalainen R. Empowering citizens for well-being and chronic disease management with wellness diary. IEEE Transactions on Information Technology in Biomedicine. 2010;14(2):456-463.
[63] Huber M, Knottnerus J, Green L, Horst H, Jadad AR, Kromhout D, Leonard B, Lorig K, Loureiro M and Meer J. How should we define health? BMJ. 2011;343:d4163. .
[64] Frantzidis CA and Bamidis PD. Description and future trends of ICT solutions offered towards independent living: The case of LLM project. Proceedings of the 2nd international conference on pervasive technologies related to assistive environments . Corfu, Greece (PETRA 09), ACM, New York, USA, 2009, Article No. 59.
[65] Center for Information Technology Leadership (CITL). The value of personal health records. Healthcare Information and Management Systems Society (HIMSS), 2008.
[66] Sassi F and Hurst J. The prevention of lifestyle-related chronic diseases: an economic framework. OECD HEALTH WORKING PAPER NO. 32. http://www.oecd.org/els/health-systems/40324263.pdf Accessed Jul 30 2013.
[67] World Health Organization. Preamble to the Constitution of the World Health Organization as Adopted by the International Health Conference, World Health Organization, New York, NY,USA, 1948.
[68] Mackey S. Towards an ontological theory of wellness: a discussion of conceptual foundations and implications for nursing. Nursing Philosophy. 2009;10(2):103-112.
[69] Oguz-Duran N and Tezer E. Wellness and self-esteem among Turkish university students. Int J for the Advancement of Counselling. 2009;31(1):32-44.
[70] Myers JE and Sweeney TJ. The Indivisible Self: An Evidence-Based Model of Wellness. The Journal of Individual Psychology. 2004;60(3):234-245.
[71] Soomlek C and Benedicenti L. Operational Wellness Model: A Wellness Model Designed for an Agent-Based Wellness Visualization System. eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED '10. Second International Conference on , vol., no., pp.45,50, 10-16 Feb. 2010.
[72] Kirsten TGJC, van der Walt HJL and Viljoen CT. Health, well-being and wellness: An anthropological eco-systemic approach. Health SA Gesondheid. 2009;14(1):1-7.
[73] Kiefer RA. An Integrative Review of the Concept of Well-Being. Holist Nurs Pract. 2008 Sep-Oct;22(5):244-52.
[74] Schuster TL, Dobson M, Jauregui M and Blanks RHI. Wellness Lifestyles I: A Theoretical Framework Linking Wellness, Health Lifestyles, and Complementary and Alternative Medicine. J Altern Complement Med. 2004;10(2):349–356.

[75] Sterling EW, von Esenwein SA, Tucker S, Fricks L and Druss BG. Integrating Wellness, Recovery, and Self-management for Mental Health Consumers. Community Ment Health J. 2010;46:130–138.
[76] Ahtinen A, Ramiah S, Blom J And Isomursu M. Design of mobile wellness applications: identifying cross-cultural factors. OZCHI '08: Designing for Habitus and Habitat. 2008:164-171.
[77] Conrad P. Wellness as Virtue: Morality and the Pursuit of Health. Culture, Medicine and Psychiatry. 1994;18:385-401.
[78] Kickbusch I and Payne L. Twenty-first century health promotion: the public health revolution meets the wellness revolution. Health Promot Int. 2003;18(4):275-8.
[79] Lorig KR and Holman H. Self-management education: history, definition, outcomes, and mechanisms. Ann Behav Med. 2003 Aug;26(1):1-7.
[80] Atkins D and Cullen T. The future of health information technology: implications for research. Med Care. 2013 Mar;51(3 Suppl 1):S1-3.
[81] Prentza A, Maglavera S and Maglaveras, N. Quality healthcare management and wellbeing through INTERLIFE services: New processes and business models. D2H2 1st transdisciplinary conference on distributed diagnosis and home healthcare, 2–4 April 2006:109-112, Arlington, USA.
[82] Maglaveras N, Chouvarda I, Koutkias VG, Gogou G, Lekka I, Goulis D, Avramidis A, Karvounis C, Louridas G and Balas EA. The citizen health system (CHS): A modular medical contact center providing quality telemedicine services. IEEE Transactions on Information Technology in Biomedicine. 2005;9(3):353-62.
[83] Mattila E, Korhonen I, Merilahti J, Nummela A, Myllymaki M and Rusko H. A concept for personal wellness management based on activity monitoring. Second international conference on pervasive computing technologies for healthcare, PervasiveHealth, 2008:32-36, Jan. 30, 2008–Feb. 1, 2008, Tampere, Finland.
[84] Patel S, Park H, Bonato P, Chan L and Rodgers M. A review of wearable sensors and systems with application in rehabilitation. Journal of NeuroEngineering and Rehabilitation. 2012;9:21, 17p.
[85] Quinn CC, Gruber-Baldini AL, Shardell M, Weed K, Clough SS, Peeples M, Terrin M, Bronich-Hall L, Barr E and Lender, D. Mobile diabetes intervention study: Testing a personalized treatment/behavioral communication intervention for blood glucose control. Contemporary Clinical Trials. 2009;30(4):334-346.
[86] Lee HJ, Lee SH, Ha KS, Jang HC, Chung WY, Kim JY, Chang YS and Yoo DH. Ubiquitous healthcare service using Zigbee and mobile phone for elderly patients. Int J of Med Inform. 2009;78(3)193–8.
[87] Fayn J and Rubel P. Toward a personal health society in cardiology. IEEE Transactions on Information Technology in Biomedicine. 2010;14(2):401–9.
[88] Honka A, Kaipainen K, Hietala H and Saranummi N. Rethinking Health: ICT-enabled Services to Empower People to Manage Their Health. IEEE Rev Biomed Eng. 2011; 4:119-39.
[89] Tang PC, Ash JS, Bates DW, Overhage JM and Sands DZ. Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. JAMIA. 2006;13:121–126.
[90] Detmer D, Bloomrosen M, Raymond B and Paul TC. Integrated personal health records: Transformative tools for consumer-centric care. BMC Medical Informatics and Decision Making. 2008;8:45.
[91] Markle Foundation. Connecting for health: The personal health working group final report, 2003, Jul 1.
[92] Connecting for Health. Common framework for networked personal health information: Consumers as network participants. Markle Foundation,

http://www.markle.org/health/markle-common-framework/connecting-consumers, 2008. Accessed 28 May 2013.
[93] National Committee on Vital and Health Statistics (NCVHS). Personal Health Records and Personal Health Record Systems, U.S. Department of Health and Human Services, Feb. 2006.
[94] Froomkin MA. The new health information architecture: Coping with the privacy implications of the personal health records revolution. UM ELSI Group for Project HealthDesign, 2008.
[95] Halamka JD, Mandl KD and Tang PC. Early experiences with personal health records. Journal of the American Medical Informatics Association. 2008;15:1–7.
[96] Pisanelli DM, Gangemi A and Steve G. Ontologies and Information Systems: the Marriage of the Century?, In: Fujita H and Johannesson (Eds.). New trends in software methodologies, tools and techniques, p 3-22, IOS Press, Amsterdam, 2002.
[97] Thorsen KAH, Eftestol T, Tossebro E and Rong C. Using ontologies to integrate and share resuscitation data from diverse medical devices. Resuscitation. 2009 May;80(5):511–6.
[98] Joshi A, Finin T, Kagal T, Parker J and Patwardhan A. Security policies and trust in ubiquitous computing, Philosophical Transactions of the Royal Society, A. 2008;366:3769-3780.
[99] Els D and De La Rey RP. Developing a Holistic Wellness Model. SA Journal of Human Resource Management. 2006;4(2):46-56.
[100] Sweeney T and Witmer JM. Beyond social interest: Striving toward optimum health and wellness. Individual Psychology. 1991;47:527-40.
[101] Myers JE and Sweeney TJ. Wellness Counseling: The Evidence Base for Practice. Journal of Counseling and Development. 2008 Fall;86(4):482-93.
[102] Saylor C. The Circle of Health: A Health Definition Model. J Holist Nurs. 2004;22(2):97-115.
[103] Strang T, Linnhoff-Popien CA. Context modeling survey. In: Indulska J and Roure DD (Eds.), Proceedings of the First International Workshop on Advanced Context Modelling, Reasoning and Management, in conjunction with UbiComp 2004, Nottingham, England, September 7, 2004, Nottingham, UK..
[104] Dey AK and Abowd GD. Towards a better understanding of context and context-awareness. GVU Technical Report; GIT-GVU-99-22; 1999. URL: https://smartech.gatech.edu/bitstream/handle/1853/3389/99-22.pdf, Accessed 4 Jun 2013.
[105] Chen G and Kotz D. A survey of context-aware mobile computing research. Technical Report TR2000-381, Dartmouth College, Computer Science, Hanover, NH, Nov 2000.
[106] Chen H, Finin T and Joshi A. An Ontology for Context-Aware Pervasive Computing Environments. The Knowledge Engineering Review. 2003 Sep;18(3):197-207.
[107] Dourish P. What we talk about when we talk about context. Personal Ubiquitous Comput.2004 Feb; 8; 1; 19-30.
[108] Soylu A, Causmaecker P and Desmet P. Context and adaptivity in pervasive computing environments: links with software engineering and ontological engineering. Journal of Software. 2009 Nov;4(9):992-1013.
[109] Dey AK, Salber D and Abowd GD. A conceptual framework and toolkit for supporting the rapid prototyping of context-aware applications in special issue on context-aware computing. Hum. Comput. Interact. J. 2001;16(2–4):97–166.
[110] Brooks K. The context quintet: narrative elements applied to context awareness. Proceedings of the International Conference on Human Computer Interaction. 2003; Crete, Greece. Lawrence Erlbaum Associates, Inc.

[111] Hervas R, Bravo J and Fontecha J. A context model based on ontological languages: a proposal for information visualization. Journal of Universal Computer Science. 2010;16;12;1539-1555.
[112] Fitrianie S, Tatomir I and Rothkrantz LJM. A context aware and user tailored multimodal information generation in a multimodal HCI framework. EUROMEDIA 2008, April 9-11, 2008, University of Porto, Porto, Portugal, p 95-103, Eurosis.
[113] Bettini B, Brdiczka O, Henricksen K, Indulska J, Nicklas D, Ranganathan A, et al. A survey of context modelling and reasoning techniques. Pervasive and Mobile Computing. 2010 Apr;6;2:161-180.
[114] Schilit B, Adams N and Want R. Context-aware computing applications. Proceedings of the Mobile Computing Systems and Applications, p 85-90, IEEE Computer Society Washington, DC, USA, 1994.
[115] Satyanarayanan M. Pervasive computing: vision and challenges. IEEE Pers. Commun., 2001 Aug;8(4):10-7.
[116] Addas S. A call for engaging context in HCI/MIS-research with examples from the area of technology interruptions. AIS Transactions in Human-Computer Interaction. 2010;4(2):178-96.
[117] Johns G. In praise of context. J Organ Behav. 2001;22(1):31-42.
[118] Viswanathan H, Chen B and Pompili, D. Research challenges in computation, communication, and context awareness for ubiquitous healthcare. IEEE Commun Mag. 2012 May;50(5):92-9.
[119] Orwat C, Grafe A and Faulwasser T. Towards pervasive computing in health care – A literature review. BMC Medical Informatics and Decision Making. 2008;8(26).
[120] Osmani V, Balasubramaniama S and Botvich D. Human activity recognition in pervasive health-care: Supporting efficient remote collaboration. Journal of Network and Computer Applications. 2008 Nov;31(4):628–55.
[121] Pulli P, Metso A and Zheng X. Ubiquitous services for senior citizens – service architecture and middleware. Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL '08. First International Symposium on , vol., no., pp.1–5, 25–28 Oct. 2008, Aalborg, Denmark.
[122] Paganelli F and Giuli D. An ontology-based system for context-aware and configurable services to support home-based continuous care. IEEE Trans Inf Technol Biomed. 2011 Mar;15(2):324-333.
[123] Catarinucci L, Colella R, Esposito A, Tarricone L and Zappatore M. RFID sensor-tags feeding a context-aware rule-based healthcare monitoring system. J Med Syst. 2012;36:3435–49.
[124] Fenza G, Furno D and Loia V. Hybrid approach for context-aware service discovery in healthcare domain. J Comput System Sci. 2012;78:1232–47.
[125] Das B, Seelye AM, Thomas BL, Cook DJ, Holder LB and Schmitter-Edgecombe M. Using smart phones for context-aware prompting in smart environments. In proceedings: Consumer Communications and Networking Conference (CCNC), 2012 IEEE , vol., no., pp.399,403, 14-17 Jan. 2012.
[126] Wongpatikaseree K, Ikeda, M, Buranarach, M, Supnithi, T, Lim AO and Yasuo Tan. Activity Recognition using Context-Aware Infrastructure Ontology in Smart Home Domain. Knowledge, Information and Creativity Support Systems (KICSS), 2012 Seventh International Conference on , vol., no., pp.50,57, 8-10 Nov. 2012.
[127] Zhang D, Yu Z and Chin CY. Context-aware infrastructure for personalized healthcare. Stud Health Technol Inform. 2005;117:54-63.
[128] Peleg, M, Broens T, Gonźalez-Ferrer A and Shalom E. Architecture for a Ubiquitous Context-aware Clinical Guidance System for Patients and Care Providers. In Proceedings of Joint Workshop on Knowledge Representation for

Health Care (KR4HC) and Process-oriented Information Systems in Healthcare (ProHealth) 2013, p 161-167.
[129] Jahnke JH, Bychkov Y, Dahlem D and Kawasame L. Implicit, Context-Aware Computing for Health Care. In: Proceedings of OOPSLA'04 Workshop on Building Software for Pervasive Computing, San Diego, CA, October 2004, position paper.
[130] Bricon-Souf N and Newman C. Context-awareness in health care: A review. Int J Med Inform. 2007;76:2-12.
[131] Jafari S, Mtenzi F, O'Driscoll C, Fitzpatrick R and O'Shea B. Measuring privacy in ubiquitous computing applications. Int J of Digital Society, 2011;2(3):547-50
[132] Uddin G M, Zulkernine M, Ahamed S I, Cat: A Context-Aware Trust Model for Open and Dynamic Systems. In: Proceeding of the 2008 ACM symposium on Applied computing, March 16-20, 2008,Brazil, 2024-2029.
[133] Khiabani H, Sidek Z M and Manan J-L (2010). Towards a Unified trust Model in Pervasive Systems. Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on , vol., no., pp.831,835, 20-23 April 2010.
[134] Ruohomaa S and Kutvonen L (2005). Trust management Survey. In: Herrmann P et al. (Eds): iTrust 2005, LNCS 3477, 77-92, 2005. Springer-Verlag, Heidelberg 2005.
[135] Lu G, Lu J, Yao S and Yip J. A Review on Computational Trust Models for Multi-agent Systems. The Open Information Science Journal. 2009;2:18-25.
[136] Krukow K, Nielsen M and Sassone V (2008). Trust models in ubiquitous computing. Philosophical Transactions of Royal Society A. 2008;366:3781-93.
[137] Belanger F, Hiller JS and Smith W. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. Journal of Strategic Information Systems. 2002;11:245-270.
[138] Guarda P and Zannone N. Towards the development of privacy-aware systems. J Information and Software Technology. 2009 Feb;51(2):337-50.
[139] Pearson A and M C Mont (2011). Sticky Polices: An Approach for Managing Privacy across Multiple Parties. Computer. 2011 Sep;44(9):60-68.
[140] Kumaraguru P, Cranor L, Lobo J, and Calo S. A survey of privacy policy languages. Workshop on Usable IT Security Management (USM 07). In SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security (New York, NY, USA, March 2007), ACM.
[141] Schaub F, Koenings B, Dietzel S, Weber M and Kargl F. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, UbiComp 2012, CASEMANS 2012 Workshop, 8 Sep 2012, Pittsburgh, PA, USA. p 752-757.
[142] Faravelon A, Chollet S, Verdier C and Front A. Enforcing privacy as access control in a pervasive context. Consumer Communications and Networking Conference (CCNC), 2012 IEEE , vol., no., pp.380,384, 14-17 Jan. 2012.
[143] Hong J, Ng D J, Lederer S and Landay JA. Privacy Risk Models for Designing Privacy Sensitive Ubiquitous Computing Systems. Human-Computer Interaction Institute. Paper 69, Aug 1-4, 2004, Cambridge, Massachusetts, USA, ACM 1-58113-787-7/04/008.
[144] Sacramento V, Endler M and Nascimento F.N. A Privacy Service for Context-aware Mobile Computing. First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm), 05-09 Sept. 2005, vol., no., pp.182,193.
[145] Wishart R, Henricksen K and Indulska J. Context Obfuscation for Privacy via Ontological Descriptions. Lecture Notes in Computer Science. 2005; 3479:276-288.

[146] Sagaran C, Dehghantanha A and Ramli R. A User-Centered Context-Sensitive Privacy Model in Pervasive Systems. Second International Conference on Communication Software and Networks (ICCSN '10.), 26-28 Feb. 2010:78-82.
[147] Jagtap P, Joshi A, Finin T and Zavala L. Preserving Privacy in Context-Aware Systems. Fifth IEEE International Conference on Semantic Computing (ICSC), 18-21 Sept. 2011:149-153.
[148] Ko H, Marreiros G, Vale Z and Choi J. A Study on Context Services Model with Location Privacy. Lecture Notes in Computer Science. 2011;6908:321-329.
[149] Chakraborty S, Raghavan K, Johson M and Srivastava M. A framework for context-aware privacy of sensor data on mobile systems. Proceedings of the 14th Workshop on Mobile Computing Systems and Applications (HotMobile '13). 2013;Article No. 11. ACM New York, NY, USA.
[150] Salah H, Eltoweissy M, Abel-Hamid A. Computational Trust for Peer-to-Peer Web Services.: Virginia Tech; 2008. URL:http://www.cs.purdue.edu/homes/fahmy/icnp2008/posters/Salah.pdf, Accessed 30 Oct 2013.
[151] Behrooz A and Devlic A. A Context-aware Privacy Policy Language for controlling access to context information of mobile users. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. 2012;94:25-39.
[152] Blount M, Davis J, Ebling M, Jerome W, Leiba B, Xuan Liu and Misra A. Privacy Engine for Context-Aware Enterprise Application Services. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 17-20 Dec. 2008;2:94-100.
[153] Ghosh D, Joshi A, Finin T and Jagtap P. Privacy control in smart phones using semantically rich reasoning and context modeling. IEEE Symposium on Security and Privacy Workshops (SPW), 24-25 May 2012:82-85.
[154] Corradi A, Montanari R and Tibaldi D. Context-based Access Control Management in Ubiquitous Environments. Third IEEE International Symposium on Network Computing and Applications, Aug.-1 Sept. 2004:253-260.
[155] Xu H (2012). Reframing privacy 2.0 in online social networks. University of Pennsylvania Journal of Constitutional Law. 2012 03;14(4):1077-102.
[156] Nykänen, P., Ruotsalainen, P., Blobel, B., & Seppälä, A. (2009). Research on trusted personal health and wellness information in ubiquitous health information space. In D. Dössel & W. C. Schlegel (Eds.), World congress on medical physics and biomedical engineering, Munchen, Germany. IFMBE Proceedings 25/XII (pp. 432–435). Berlin: Springer.
[157] Seppälä A and Nykänen P (2011). Contextual analysis and modeling of personal wellness. In: Proceedings of the International Conference Knowledge Engineering and Ontology Development (KEOD ’11), J. Filipe and J. L. G. Dietz, Eds., pp. 26–29, Paris, France, October 2011.
[158] Blobel B, González C, Oemig F, Lopéz D, Nykänen P and Ruotsalainen P. The role of architecture and ontology for interoperability. Stud Health Technol Inform. 2010; 155:33-39.
[159] Ruotsalainen P, Blobel B, Nykänen P, Seppälä A and Sorvari H. Framework model and principles for trusted information sharing in pervasive health. Stud Health Technol Inform. 2011;169:497-501.
[160] Golafshani N. Understanding Reliability and Validity in Qualitative Research. Qualitative Report. 2003, 8:597-606.
[161] Whittemore R, Chase SK and Mandle CL. Validity in Qualitative Research. Qual Health Res. 2001 Jul;11(4):522-37.
[162] Tracy S. Qualitative Quality: Eight "Big-Tent" Criteria for Excellent Qualitative Research. Qualitative Inquiry. 2010;16(10):837-51.

[163] Morse JM, Barrett M, Mayan M, Olson K and Spiers J. Verification strategies for establishing reliability and validity in qualitative research. International Journal of Qualitative Methods. 2002;1(2); Article 2.
[164] International Medical Informatics Association (IMIA). IMIA Code of Ethics for Health Information Professionals, 2011. http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf Accessed Sep 11 2013.

Original publications

Chapter 8
Collaborative Approach for Sustainable Citizen-Centered Health Care

Pirkko Nykänen and Antto Seppälä

Abstract Health care systems are in transition to citizen-centered care with focus on prevention, proactive and personalized services and healthy lifestyles. Innovative technologies enable citizens' empowerment and allow them to manage their complete health and wellness. Citizen-centered tools collect life-long cross-institutional information and data from health care providers and citizens. From the health care organizations viewpoint the new paradigm implies changes in the ways how the services are produced, how they are offered for use and in the contents of the services. Research with the citizen-centered health paradigm has been active and many significant results have been achieved, for instance improvements in citizens' lifestyle, weight loss, reduction of the duration of hospitalization, better accessibility of health related information and improved communication between the care providers.

Based on our literature review we present in this chapter the approaches, achievements, barriers and challenges of citizen-centered health paradigm. We propose a new innovative approach to build the next generation, collaborative health information space that links the care providers and citizens together and helps them to access the distributed health resources any time anywhere. The visional, sustainable citizen-centered health environment offers means to gradually migrate from the current situation to a citizen-centered care environment where citizens have a participatory role in health care activities.

Keywords Citizen • Centered health care • Sustainable • Personal health record • Personal health systems • Social media • Collaborative health care environment

P. Nykänen (✉) • A. Seppälä
School of Information Sciences, Centre for Information and Systems, eHealth Research, University of Tampere, Tampere, Finland
e-mail: Pirkko.Nykanen@uta.fi

N. Wickramasinghe et al. (eds.), *Critical Issues for the Development of Sustainable E-health Solutions*, Healthcare Delivery in the Information Age,
DOI 10.1007/978-1-4614-1536-7_8, © Springer Science+Business Media, LLC 2012

8.1 Introduction

Health care systems around the world are facing challenges especially with availability, costs and quality of health services. Personal Health Systems 2020 Support Action (Codagnone 2009) has recognized 8 challenges that health care systems face in the future: Population ageing and other prevalence related trends (e.g. obesity), increasing income, consumerism and demand for equal and fair access, increasing capacity to cure, overshooting or mismatch in resource allocation, fragmentation and overspecialization, inflation through unnecessary costs, and fat administration. Citizens' awareness is one challenge; citizens are aware of their own health and are willing to choose services based on personal needs and preferences (Monteagudo and Moreno 2007; PricewaterhouseCoopers Health Research Institute 2005; Detmer and Steen 2006). Many of these current challenges can be solved by using ICT solutions and by developing new services that can match the organizational and structural changes in health care area (Codagnone 2009; PricewaterhouseCoopers Health Research Institute 2005; Teperi et al. 2009; Varshney 2007; Wartena et al. 2009; Hill and Powell 2009).

There are programs ongoing worldwide with the purpose to meet these challenges. We can identify some major issues that are common to most of these national health IT initiatives (McConnell 2004; Jha et al. 2008; Aaltonen et al. 2009; eHealth roadmap – Finland 2007). A general objective is to have nationally access the core patient data, i.e. patient's diagnoses, medication data, examinations, care actions and patient risk data. There is also a widely shared understanding and agreement on the contents of these core patient data. The international trend is to document the core patient data in a structured manner and for this purpose headings, classifications, nomenclatures and agreed coding systems are used. Other major issues are use of standards and secure authentication and identification of the users.

Patient data is stored locally or regionally, there are very few attempts to build a centralized national patient data archive. An exception is Finland where a national digital patient data archive is under development (eHealth roadmap – Finland 2007). A major focus generally with patient data is on easy access when and where data is needed. A clinical path, or a treatment chain can build the connection between the data entities in various systems (Adler-Milstein et al. 2009).

An important component in these national programs is a secure data transfer channel to enable patient data exchange between health care organizations and professionals, and very recently also between health professionals and patients. In most countries Internet is considered secure enough, but in some countries, e.g. in UK and Sweden special telecommunication networks have been established for health care (Iliakovidis et al. 2005; Malmqvist et al. 2005).

In most countries the national programs and initiatives put special emphasis on citizen services. The citizens should have access to their own health related data and information. There are some good examples already on these systems, e.g. in USA and UK which offer for their citizen's access to patient data which is stored in their

own data bases (Aaltonen et al. 2009; Iliakovidis et al. 2005; Basch 2005). There are also commercial products already available for citizens, e.g. Health Vault and Google Health, that offer citizens tools to integrate their own health data with other wellness information for their individual needs. These examples demonstrate the ongoing shift from an organization-centered health care to citizen-centered health care where the focus is on prevention, proactive services, healthy lifestyle and personalized services for citizens.

8.2 Citizen-Centered Health Care Paradigm

Current health care systems are organization-centered and patient care processes are static and designed mostly from the physicians' viewpoint. Patient care is focusing on treatment of diseases and care is organized by specialty or intervention. Care is composed of sequences of care episodes given by various providers and this situation does not really support multi-professional and collaborative care. There is lack of communication between the participants and also many delays and queues in the processes (Teperi et al. 2009; Koop et al. 2008; Pratt et al. 2006; Ohashi et al. 2010).

In the citizen-centered care (CCC) paradigm health care systems should transform their processes in such a way that the individual citizen is placed in the middle of health care processes. Health is seen in a more holistic way where the focus is on individual's complete wellness, covering health, diseases, care, prevention, wellness and healthy lifestyle. Essential is that citizen-centered care will enable the citizen to take an active part in his/her health care processes throughout his/her lifetime anytime and anywhere (Teperi et al. 2009; Wartena et al. 2009; Pratt et al. 2006; Ohashi et al. 2010; Nykänen 2008; Tang and Lansky 2005).

The core of the citizen-centered care paradigm is to focus on preventive care, on proactive services, on early detection and diagnosis to ensure citizens personal wellness. Thus, there is a need for new citizen-oriented services covering health promotion, health maintenance and citizen education and empowerment Also health care providers should be open and able to communicate and give citizens more information on their health and wellness related issues (PricewaterhouseCoopers Health Research Institute 2005; Wartena et al. 2009; Koop et al. 2008; Ohashi et al. 2010; Continua Health Alliance 2005; Kolitsi and Cabrera 2007; Berry and Mirabito 2010).

Citizen-centered care creates a need for new kinds of interoperable and sharable networks of services which can also include other actors than health care providers. These networked services create new challenges for health care systems and care processes should become multi-professional, decentralized, distributed, easily accessible and based on personalization of care. When patient care is shared in the network of service providers there is a need to share also the patient data and care

management. Currently patient data is fragmented and stored in distributed data bases and it is not easily accessible when and where needed (Varshney 2007; Pratt et al. 2006). Shared care processes need interoperable information systems to handle increasing number of information sources and participants in the patient care (Koop et al. 2008; Ohashi et al. 2010).

Since citizen-centered care model is based on the networked services and shared care management there is a need for extended communication and co-operation through processes to ensure comprehensive services. Different participants in care processes need real-time reliable information to be able to make justified decisions. The amount of health related information is increasingly growing and it is critical to have access to citizens' histories, medications, test results and clinical records but also to their lifestyle choices, behaviors and personal information (Tang and Lansky 2005; Kolitsi and and Cabrera 2007). A requirement for implementation of the citizen-centered care model is empowerment of the citizens. Citizens are not anymore passive users of services but active participants in the care processes who take responsibility of their care (Pratt et al. 2006; Kolitsi and Cabrera 2007).

Current health care services are fragmented and therefore the citizens now need to act themselves as care integrators who are responsible for the completeness of care (Monteagudo and Moreno 2007; Pratt et al. 2006).Citizen empowerment is seen as a potential tool to cut down costs in health care, because much of the responsibility is moved to the citizen (Monteagudo and Moreno 2007; PricewaterhouseCoopers Health Research Institute 2005; Wartena et al. 2009) and maintenance of wellness and prevention has better return of investment than treatment of a disease after diagnosis (Continua Health Alliance 2005; Berry and Mirabito 2010; World Health Organization (WHO) 2006).

Increased empowerment of citizens and their collaboration with service providers may improve the quality of care through improved lifestyle choices and health behaviors, better disease management, improved care coordination, and following better care recommendations. High quality information is needed to empower the citizens to make effective decisions and choices. Missing information can be damaging to citizens, their relatives and proxies and also to health care providers (Monteagudo and Moreno 2007; Varshney 2007; Center for Information Technology Leadership (CITL) 2008).

In citizen-centered care model citizens should be able to access health care from and at their homes and in everyday life, instead of visiting health care organizations. Technology makes it today possible to support the citizens' activities outside the care provider networks. These activities vary from life style and self health management to improving the life of citizens as well as managing chronic diseases (Continua Health Alliance 2005; Kolitsi and Cabrera 2007). For example chronic diseases related to the lifestyle are one of the main reasons for diseases and deaths in the developed countries (World Health Organization (WHO) 2006; Mattila et al. 2010). It would be very beneficial and cost-effective to help citizens to better manage their chronic diseases and possibly prevent these diseases by offering citizens information and support for prevention and healthy lifestyle.

8.3 Examples of Citizen-Centered Care

8.3.1 Personal Health Record

To implement the citizen-centered care model we need new tools for extended communication, collaboration and to support citizens' activities concerning their health and wellness. One of the existing tools is the personal health record (PHR).

Markle Foundation (2003) has defined attributes for PHR systems:

- Each person controls his or her own PHR,
- PHRs contain information from one's entire lifetime including information from all health care providers,
- PHRs are accessible from any place at any time,
- PHRs are private and secure,
- PHRs are transparent. Individuals can see who entered each piece of data, where it was transferred from and who has viewed it,
- PHRs permit easy exchange of information across the health care system.

These characteristics try to ensure the credibility of PHR. This definition is widely referenced to (See e.g. Monteagudo and Moreno 2007; Detmer and Steen 2006; Tang and Lansky 2005; Pagliari et al. 2007).

In the European Union research on personal health systems (PHS) is seen important. The personal health systems aim at improving and preserving the health of citizens outside the institutional care (Kolitsi and Cabrera 2007). The research focuses on wearable and portable systems, necessary tools for users, on the convergence between ICT and other technologies (e.g. biomedical sensors, micro- and nanosystems) and on connecting citizens with health care networks rather than on connecting health information systems together (Codagnone 2009).

In 2008 there were 100–200 PHR solutions already available in the USA (Center for Information Technology Leadership (CITL) 2008). The scope and nature of functions, content and information sources vary between different PHR systems but the basic idea is to give citizens access to their own health and wellness information, provide an integrated view of health and wellness including status, medical and treatment history and interactions with the providers (Markle Foundation 2003; Halamka et al. 2008; Connecting for Health 2008).

PHR systems can be divided into three different approaches. The simplest one is a standalone PHR which enables citizens to collect their information into a PHR which can be a paper-based, a portable device, a personal computer or a web based application. Standalone PHR is not connected to any other systems. The tethered approach allows citizens to view their own information from the health care providers electronic health record (EHR) and citizens do not have total control of their records. Interconnected PHR enables citizens to collect health information from multiple sources, enter their own entries, share information with different parties and totally control their own information. Interconnected PHR can produce more benefits to all

stakeholders because of its interoperability with other systems (Tang and Lansky 2005; Tang et al. 2006; Detmer et al. 2008; Nykänen et al. 2009).

It is evident that PHR systems will play a major role in the change of health care systems to citizen-centered care model by empowering citizens and making health information available when and where it is needed. PHR can be seen as a technology that can improve health care delivery and the quality of care, lower the costs and help citizens' empowerment (Center for Information Technology Leadership (CITL) 2008; Markle Foundation 2003; Connecting for Health 2008; AHIMA e-HIM Personal Health Record Work Group 2005; National Committee on Vital and Health Statistics (NCVHS) 2006; Froomkin 2008). Citizens are creating (e.g. by using sensors, devices, and health diaries) and controlling their own health information, which enables the PHR model to be citizen-centered.

PHR is usually considered to include set of tools which are designed to help citizens to collect, access, coordinate, share and store their lifelong personal wellness and health information. PHR can also include decision support functions to help citizens to manage and co-ordinate their own health and wellness, and to track and manage health activities through their lifetime. Basically PHR is helping citizens to create an integrated and complete view of their health and wellness (Detmer and Steen 2006; Markle Foundation 2003; Connecting for Health 2008; Tang et al. 2006; Detmer et al. 2008; National Committee on Vital and Health Statistics (NCVHS) 2006).

The information and data in PHR is life-long and cross-institutional and it covers clinical data and information from different health care providers but there can also be citizens' own entries, observations, measurement data etc. In PHR citizens can collect their own information and manage it and possibly share it between different parties, but it is not designed to substitute the information in health care providers' information systems and in EHRs and use of PHR will not remove the legal obligations for recordkeeping from health care providers (Markle Foundation 2003; Connecting for Health 2008; Tang et al. 2006; AHIMA e-HIM Personal Health Record Work Group 2005).

The number of actors (e.g. sensors, advanced technology solutions) and stakeholders is increasing in the personal health ecosystem. Ecosystem term refers to the comprehensive system composed of PHR, integrated devices and sensors, and relevant actors and information systems in the personal health care environment. The ecosystem creates much information and data and the need for interoperability is growing (Wartena et al. 2009). Today, most sensors and information systems communicate differently and their transport mechanisms may vary. It is very challenging to create an interoperable personal health ecosystem with all of these different actors. To achieve true interoperability between different systems both structure (syntax) and meaning (semantics) of the data must be defined. Currently there are no proper standards or methods to enable real interoperability and data transfer between EHR and PHR systems (Wartena et al. 2009; Detmer et al. 2008). Without interoperability PHR systems will only be isolated information islands with limited value. PHR systems need to be integrated together with different health information systems. In the future PHR systems may even be so advanced that they have

connections also to the health care delivery systems and are integrated seamlessly with other systems (Tang et al. 2006).

PHR puts new kinds of pressure also for citizens. Citizens may consider use of PHR inconvenient, difficult, or costly (Monteagudo and Moreno 2007). Citizens should be educated about PHR so they can understand the benefits of PHR and how citizen-centered health care will affect them (Tang et al. 2006). Citizens have to adopt their new roles and responsibilities related to their own health care. It is necessary to define how PHR can be part of citizens' lives and wellness management. PHR can only be successful if citizens understand potential benefits and are ready to maintain and coordinate their health information and activities with health care providers. There is also need for governmental guidelines and decisions in health care to find ways to support or reimburse the citizens' cost on using PHR systems.

8.3.2 Current Domains for Citizen-Centered Care

Chronic diseases related to lifestyle are major risks in developed countries. According to World Health Organization (WHO 2006) 70–80% of health care expenses are caused by chronic conditions. Lifestyle choices and behaviors are important for managing and preventing chronic diseases. The seven leading risk factors account for almost 60% of disease burden in Europe (World Health Organization (WHO) 2006). These factors are high blood pressure, tobacco, alcohol, high blood cholesterol, overweight, low fruit and vegetable intake and physical inactivity. All of these risk factors are closely related to lifestyle and behavior and can be managed and possibly minimized through better behavior and education. Prevention and better control of noncommunicable diseases are ways to improve the quality of life and well-being of citizens (World Health Organization (WHO) 2006).

Different tools for lifestyle, behavior and wellness management are part of the citizen-centered care model. These tools enable citizen empowerment and make it possible to manage citizens' complete health and wellness. Citizen empowerment is needed to ensure success of new models for disease management. New disease management models should help citizens to manage their complete wellness and actions to prevent diseases but also enable managing already existing diseases.

Rapid development of technology and growth of Internet use has made it possible to create pervasive health services. The goal of pervasive services is to improve citizens' lives through proactive and intelligent computing environment. Pervasive services can be used to monitor or support citizen's daily life, e.g. through sensors and devices citizens' activities (e.g. sleep, physical activity and energy expenditure) can be followed automatically and thus possibly detect emergency situations (e.g. falls, heart rate, blood glucose level) and risky situations or behaviors. Also behavior and emotion monitoring tools are being developed which can help to create more personalized care and early detection of new diseases and emergencies (Osmani et al. 2008; Mattila et al. 2008; Pulli et al. 2008). Already many mobile phones include tools to track physical activity and nutrition. Wellness systems

include solutions to follow physiological measurement and development of health. Examples of developed tools are wearable devices for activity monitoring (Mattila et al. 2008), wellness diaries (Mattila et al. 2010), ECG measurement solutions for detection of cardiac syndromes (Fayn and Rubel 2010; Lee et al. 2009), tools for diabetics to measure blood glucose (Lee et al. 2009; Quinn et al. 2009), home monitoring systems (Prentza et al. 2006) and personal health records.

Home care offers many possibilities for managing chronic diseases. Continuous monitoring at home with information systems can help to improve quality of life and care. A modular home care system tailored for citizens suffering from different chronic diseases was developed in the Citizen Health System (CHS) project (Maglaveras et al. 2005). The CHS system offered citizen-focused services for measurements, communication with providers, education and interactive sessions with medical personnel to transmit measurement data or to ask advice. The CHS system supported monitoring of patients suffering from heart diseases, diabetes or obesity. The CHS project had very promising results concerning weight-loss and reducing hospitalization of heart failure patients. The CHS system was well-accepted by the citizens and physicians.

The EPI-MEDICS is a portable, intelligent and personal self-care system designed to support citizens' own management of cardiac status by providing personal ECG monitor to be used on-demand (Quinn et al. 2009). The system was designed to enable citizens to import recorded information easily to be used by health care professionals. The EPI-MEDICS was very well accepted by the providers and patients who felt more secure with such a system.

Wellness diary (WD) is an example of a mobile application which is designed to support citizens' actions on wellness management (Mattila et al. 2010). Mobile technology is suitable for wellness and self management because people usually carry the technology with them all the time, and the technology enables constant updating and immediate usage despite of the location or time. WD is a self-monitoring journal which enables recording of health and behavior related observations (e.g. activity, weight, smoking, eating, and blood pressure) which helps self-observation and behavior management. WD also gives feedback to users concerning their actions and behavior. Mattila et al. (2010) concluded that WD works quite well when it assists intervention and users get support from experts. But, users need to be properly educated about the possible benefits of using WD and self-observing. The long-term use of WD and its benefits seems to be connected to the motivation of patients and external support. Also users need interesting features which engage users, maintain their motivation, helps recovery and give more feedback. Even simple personalization of WD could help to meet the different needs of different user groups.

Aging population uses a lot of health care system resources. Independent and autonomous living is seen as a good way to reduce care costs, increase quality of life and improve efficiency of health care. Ambient assisted living (AAL) is an approach to help elderly people to manage living at home by offering them new ICT-based solutions e.g. for remote monitoring and emergency alarms and messages. AAL and independent living are trends which are affecting strongly on elderly care and transforming it towards citizen-centered care.

ICT-based applications give new ways for communication between elderly people and health care providers. The Internet gives access to health information and also enables social-networking which may give senior citizens new social relations concerning their needs and experiences about health and may offer more social activities and reduce their feeling of isolation (Frantzidis and Bamidis 2009). Needs and skills of elderly people are quite heterogeneous and new services have to be personalized according to their needs. Independent living is one example of citizen-centered care where the needs of the citizens' should be the starting point for planning of the care.

In the European Union ambient assisted living research has focused on physical and mental status of elderly people and to support independent living with the purpose to reduce costs, improve efficiency and improve quality of life by reducing institutionalization. The proportion of elderly people is growing and it is a challenge for health care systems. An example of independent living research is The Long Lasting Memories (LLM) project which combines tele-monitoring services and mental and physical training to improve detection of threats, to improve self-esteem of senior citizens and to reduce mental problems. It is based on smart home solutions and personalized training. The LLM project uses sensors to monitor the use of electronic appliances and citizens' movement to detect changes in regular movement patterns and possible emergencies (Frantzidis and Bamidis 2009; The Long Lasting Memories 2010).

The possibilities of mobile technology and broadband connections have been studied in many research projects (Frantzidis and Bamidis 2009), e.g. the AttentiaNet project which focused on independent living and reduction of social isolation, the OLDES project which focused on medical sensors and modern ICT to study lifestyle of elderly and how to improve their life quality and the ENABLE project with the focus on the needs of elderly people suffering from Alzheimer disease. ENABLE developed new services to enhance citizens' coping in daily living and components to improve memory and communication of the citizens.

Research in these domains with citizen-centered health paradigm has been active and many significant results have been achieved, e.g improvements in citizens' life style, weight loss and reduction of the duration of hospitalization. An important result from the elderly users is that they have felt more secure at home when they have had a supporting personal health system available. These results show that personal health systems may bring important benefits for the citizens and be cost-effective in the health care environment.

8.3.3 Citizen-Centered Care from the Health Care Service Provider's Viewpoint

The citizen-centered paradigm from the health service provision viewpoint means that health service providers do need to consider and analyze the citizens' needs for services and to develop services that fulfill these needs. Despite of this change in focus,

the public and private health care institutions still most likely are in the future the major players and funders of health care services, though it can be expected that governments are forced to reduce the amounts of health care funding during time. This results in that fragmentation increases both across tiers of governments and within the health care service providers (GPs, primary care, secondary care) and this results in varying quality of care (Codagnone 2009; European Commission et al. 2006).

In this situation technology confident users and those who have enough economical capacities are able to buy personal health services available at consumer electronics market. More traditionalist wealthy users pay for high quality services from private organizations and those with less wealth queue for the publicly funded services adapting themselves to varying quality and waiting lists. The elderly and chronically ill may not in the future receive all services they need in the same manner as today, but the citizens will have technical devices like robots or ambient intelligence for monitoring at home to help them in long term care and rehabilitation. These citizen-services are funded by the public health organizations but their use may be controlled. The use may demand from the citizen in the future that she or he fully adopts healthy lifestyle guidelines and rules to achieve the treatments and care funded with the tax money (Codagnone 2009; Ganesh 2004).

From the health care organizations viewpoint a shift to citizen-centered care implies changes in the ways how the services are produced, how they are offered for use and finally in the contents of the services. Essential change that needs to be implemented is the extension of an organization-centered EHR with an integrated personal health record (PHR) in such a way that care provided by the health organizations, care provided by e.g. third sector actors and also the citizen's own notes, diaries and measurements from the citizen's own personal health systems are covered (Detmer et al. 2008). This kind of personal health record can improve the quality, completeness, depth and accessibility of health information and enable communication between patients and providers.

8.4 The Drivers, Barriers and Issues to Consider in Sustainable Citizen-Centered Care

8.4.1 Drivers for the CCC-Model

Current problems with accessibility, costs and quality of health care are encouraging health care systems to find more efficient ways of delivering services (Hill and Powell 2009). The cost of health care has been steadily growing proportion to GDP since the 1980s (PricewaterhouseCoopers Health Research Institute 2005) and population in Europe and USA is growing older and maintaining reasonable level of health care systems is becoming harder. As the number of retirees is growing and fewer clinicians are available there is a need for more effective use of resources (Codagnone 2009; Teperi et al. 2009; Varshney 2007; Wartena et al. 2009; Hill and Powell 2009).

Health care has been very heavily based on labor, knowledge, skills and time, today innovative. Innovative technologies make it possible to create new productive services and possibly reduce the need for massive amounts of labor and time. Diagnosing diseases, creating treatment plans, educating patients, record keeping, and communication are major time and labor consumers in health care which possibly can be enhanced by using innovative technologies and standardization (Berry and Mirabito 2010).

Health promotion and preventive services are important drivers towards citizen-centered care. They have better economical value through the ability to reduce costs by promoting healthy life style, by preventing diseases and by maintaining health than the traditional disease treatment and interventions (Continua Health Alliance 2005; Berry and Mirabito 2010; World Health Organization (WHO) 2006). Health care systems are also trying to reduce hospitalization and institutionalization by implementing intelligent home care and independent living services supported by technological solutions and by improving organizational care processes (Prentza et al. 2006; Maglaveras et al. 2005; Frantzidis and Bamidis 2009).

Technology is advancing rapidly and different sensors and devices give possibilities for citizens to track and manage their own health and wellness (Mattila et al. 2010; Osmani et al. 2008). Citizens are aware of their own health and are willing to take more responsibility of their own health (Detmer and Steen 2006). Health providers are also empowering citizens by providing them health information and giving them more responsibilities concerning their own health (Monteagudo and Moreno 2007; Wartena et al. 2009). Technological solutions and the Internet are enabling citizens to share their own health related information through different communication channels. Citizens can share their experiences and ask advices in social networks and they are very active in these today (Frantzidis and Bamidis 2009).

In the citizen-centered care (CCC) collaboration between different health care providers is necessary to enable shared, comprehensive health care. Health professionals should be able to communicate with each other and create networked services with shared care management. Different participants in the care processes need real-time reliable information to be able to make justified decisions.

Citizens' needs, preferences and skills are very heterogeneous and thus the health care delivery model needs to be very flexible and adaptable and based on individualization and personalization. Citizens need different kinds of services and support depending on their personal situation and needs. In some cases they need only a short consultation, sometimes more support or thorough advice and these can be provided by a doctor, a network of medical professionals, a nurse, a non-medical professional or by the peer support groups from the social media (Berry and Mirabito 2010). Citizen-centered care paradigm also very clearly implies the possibility to develop tailored services based on the personal needs.

From health care organizations viewpoint it is important that they install more advanced information systems which can communicate with the information systems infrastructure. Interoperability of the information systems is the key issue here. Security, privacy and confidentiality of patient data have to be ensured also in the citizen-centered care model to achieve citizens' trust on the services.

8.4.2 Barriers for the CCC-Model

The barriers for citizen-centered care (CCC) paradigm are many, mostly they are due to the current, organization- or even hospital-centered care paradigm. For the citizen-centered care the concept and processes of health care need rethinking and reengineering. In a study (Detmer et al. 2008) the following factors were identified to be the major barriers for citizen-centered care:

- Health care system culture and incentives covering physician patient autonomy hinder implementation of the CCC paradigm. Also the responsibilities of various health professionals have been tightly determined and there are concerns about liability risks, if the situation changes.
- Consumers do have concerns abo security and confidentiality of their health related data, citizens are not convinced on the confidence and trust in the changing situation.
- There is lack of technical standards for interoperability including data integration standards, common core data sets, consumer terminologies, authentication and identification processes, security and privacy standards and certification. Most existing CCC solutions are tailored and very context-dependent, and thus vulnerable for changes.
- There is lack of health IT infrastructure in many countries, mostly due to the high enterprise cost of data integration, and the mediating structures between various information systems are missing.
- Citizens have concerns about equity and usability of CCC systems and they are worried about the digital divide, existence of a racial and socio-economic disparity gap.
- There are suspicions on value realization which refers to that ICT investments in health care usually require justification based on quantifiable benefits in terms of avoided cost, improved efficiency or increased revenue. The health IT business needs to take into consideration the infrastructure and labor costs for implementation, as well as ongoing system support costs. The CCC-model with integrated PHRs is a difficult business case for cost-benefit justification, due to the lack of empirical evidence in health care and informatics literature to quantify the PHR value proposition. While many of the perceived PHR benefits accrue to citizens, it is not clear that they are willing to pay or subsidize the cost of PHRs. Although surveys show substantial numbers of citizens indicating their willingness to pay this has not yet been demonstrated in practice. Benefits such as citizen and patient satisfaction, improved communication and citizen engagement are not easily quantifiable.
- There is uncertainty on the market demand because CCC-model with integrated PHRs offer both significant potential for users and a high degree of risk for potential investors.

Lopez (2007) identified the following barriers for the CCC-model in a study: Incompleteness of the existing technical infrastructure, heterogeneity of the citizens in attitudes and knowledge, slow migration from the paper-based systems to digital systems in health care, technical difficulties in system integration due to application

program interfaces, need for reengineering of work processes and procedures and concerns about data security and data privacy.

Many studies have identified critical factors for adopting electronic health records generally (Ash and Bates 2005; James 2007; Lorenzi et al. 2009) and most of these result in the following items: User attitude towards information systems, workflow impact, technical support, interoperability, expert support and communication among users.

These factors are evidently critical also for adoption of PHRs and citizen-centered care paradigm. To overcome these factors it is important to define and design the information models and data structures in such a way that they support adoption of a PHR, and redesign the underlying processes in the framework of the citizen-centered care paradigm. The PHR software architectures should be designed to implement citizen-centered processes and data and information models.

A very important concern with PHRs and citizen-centered care is the privacy and security risks. Citizen's health related data is confidential and needs to be protected from an unauthorized access and disclosure. With PHRs security and data protection issues need special attention as the citizen's health data may be in a distributed storage in a network of actors and access to that data need to be legally protected.

8.4.3 New Approaches to Consider

An innovative approach is needed to build the next generation, semantically enriched, collaborative health information space that covers both organization-centered and citizen-centered paradigms and EHR and PHR concepts respectively. The collaborative space should facilitate all stakeholders, health care providers, health professionals, patients and citizens to link, dynamically discover, effectively combine, easily and safely access the distributed health resources, data and information independent where they are provided, or needed.

An integrated PHR model is still a theoretical framework for citizen-centered health care. We need an interoperable network for new channels of communication and care management. And this points to a new tool that is clearly broader than the legal record of any provider. As traditional roles and relationships between citizens and different parts of health care delivery and financing system are fundamentally altered by a more citizen-centered framework, stakeholders may realize a variety of new benefits from interaction with PHRs.

The recent innovations in collaborative environments and social media research (Hawn 2009; Halonen 2010) can bridge the information, knowledge and collaboration gap currently existing in health care services provision and use. Collaborative environments hold considerable potential value for health care organizations because they can be used to reach stakeholders, aggregate information and leverage collaboration (De la Fuente and Ros 2009; Boulos and Wheeler 2007; Kaplan and Haenlein 2010). The collaborative environments research results support the development of a conceptual architecture that will facilitate interactive connectivity between the

available health data and health information sources such as data bases, digital archives, literature or Internet for gathering and sharing adequate knowledge for making decisions in citizen-centered care. Furthermore, these advances support development of a user friendly, collaborative decision making environment.

As more and more patients already use collaborative environments and social media to track their health conditions and care, health care organizations have an opportunity to interact with the members of these online communities and to leverage data sets to inform new treatments and care pathways. Hospitals are increasingly using social media for promotional purposes and to gauge citizens' experiences with their organizations, e.g. in USA many hospitals have a social media and social networking presence to market their services and communicate to stakeholders (Hawn 2009).

In e-Business and e-Commerce more and more companies apply social media (Kaplan and Haenlein 2010) because there are many technical tools available already to support this. Social media like Facebook, LinkedIn and Twitter consist of user profiles, connections between friends and colleagues and they support communication. All these networks establish the awareness of who is there and what are they doing, they enable communication from many to many, instead of from one to one (Hawn 2009). These tools are familiar and popular to the general public, citizens, they are also easy to use and cheap to purchase, or even free to access.

The collaborative environments and social media approach offers many possibilities for citizen-centered health. Our vision from the collaborative, sustainable citizen-centered health is presented in Fig. 8.1. The vision presents a collaborative environment without borders and it is based on two collaborative virtual health spaces: (1) the citizen's personal health space, and (2) the health care organization's regulated and legally controlled health space. These two spaces build together a collaborative health environment.

The citizen's personal health space is completely controlled, maintained and managed by the citizen himself, using the tools that seem appropriate to his situation and are usable and useful for his purposes and accessible in his situation. The health organization's health space contains patient data and information which is collected and documented by health professionals in the EHRs and other relevant health information systems during the citizen's care episodes and visits. This space is for the health professionals and administrative purposes and it is legally regulated and controlled by the health organization. Citizen does not have direct access to this health space but he can link or copy his own data and information to his own personal space. This communication is one-way; the citizen cannot transmit any information from his personal space to the health organization's space. However, the citizen can give access to the health organization to the citizen's own health space if he sees this useful and beneficiary. The social collaborative environment builds thus a platform that enables communication and sharing of data and information.

Future health care, Health 2.0, is participatory. The services are enabled by information, information systems, and the community of actors that is created and collected around a person's health and wellness. This community is composed of all

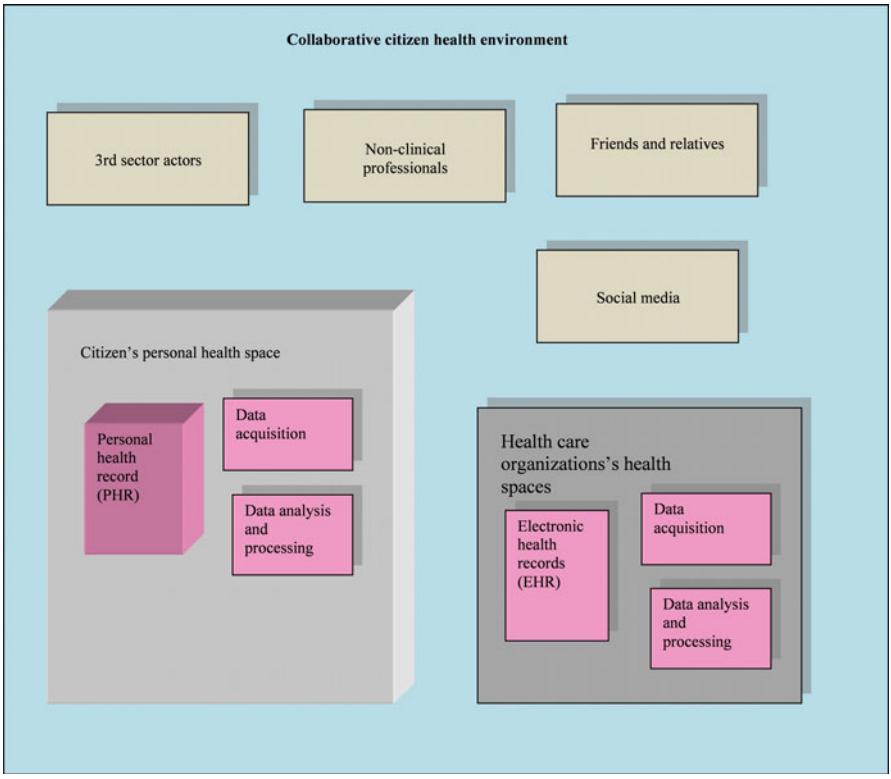


Fig. 8.1 Vision on collaborative, sustainable citizen-centered health

relevant actors needed for prevention, health care and wellness. The person himself, as a patient, as a citizen, is an active participant in this community. Thus the citizen is reshaping the health care system according to his needs and situations. These kinds of new approaches in health care change the relationship between the care givers and the care receivers.

8.5 Summary and Conclusions

Health care systems are in a transition phase, they are progressing from an organization-centered health care to a citizen-centered care, and this implies many changes on our current health care services provision, delivery and use.

Citizen-centered health care paradigm with personal health record (PHR) and personal health systems (PHS) create many challenges for health care. Froomkin (2008) found four elements of the use of PHR that create major changes in health care:

- Viewing the citizen and devices controlled by the patient build important sources of health-related data,
- Giving the citizen much greater control over health information,
- Moving personal data storage and/or queries based on personal data towards Internet-based applications,
- Permitting, even encouraging, citizens and patients to share health data via informal social networks.

Continua Health Alliance (2005) identified four considerable benefits from citizen empowerment and new models of health care:

- Improvements in citizen's lifestyles, current poor health lifestyles dramatically increase population risk for disease,
- Early diagnosis and detection reduces care costs, much costs come currently from waiting to intervene until after disease is present,
- Citizen empowerment helps the low risk populations to remain healthy by modifying personal health behaviors,
- Return on investment from wellness-focused programs has been achievable and dramatic.

CCC-based system beneficiaries are usually individual citizens but other stakeholders may also benefit from their use (Tang et al. 2006) because CCC-based systems support health care decisions and continuity of care across time and providers (National Committee on Vital and Health Statistics (NCVHS) 2006). Personal systems may also save time and money and increase the quality of care, because they may decrease duplicate testing, help to access patient records, reduce drug adverse events and improve preventive care and health management (Markle Foundation 2003; Pagliari et al. 2007).

CCC-based systems may produce benefits to individuals who wish to stay fit or are at risk and wish to maintain normal health status, to chronically ill patients, to individuals who want to live independently outside care institutions and health professionals (Codagnone 2009). The main benefit to all citizens is the access to their health information and data which they can use to support their wellness activities, e.g. management of chronic diseases, prevention, life style choices. These systems also have the potential to improve communication between the citizen and her health care provider and make it possible to create ongoing connection between the citizen and the provider so they can have a continuous care process instead of an episodic, disease focused one. Communication makes it easier for citizens and providers to ask questions, to make appointments, to request refills and referrals, and to report problems (Pagliari et al. 2007; Tang et al. 2006).

Citizen-centered care paradigm has a lot of potential for benefits but these will only be realized with widespread use (Tang et al. 2006). The health care workflows need to be changed to personalized and citizen-centered (Clarke and Meiris 2006). Partnership is essential between all stakeholders and this means new ways of making care decisions, new roles for professionals and reengineered workflows (Kolitsi and Cabrera 2007).

It is important, however, to notice that CCC-based applications are currently still a very small niche market and this is due to the barriers and gaps of socio-economic, institutional and cultural nature that the technological research will not solve by itself. The success of the approach is not only dependent on technological factors but a lot of work is needed to face the social and cultural obstacles. Policy initiatives, legislation and institutional reengineering, inter-institutional and interdisciplinary collaboration as well as support to implementation and deployment are needed to create the correct structure of incentives across the entire value chain, and to identify and sustain new business and funding models. From the health care perspective we need to increase efforts in the preventive field, to reduce healthcare fragmentation and to increase the delivery of integrated care to better inform and educate users and overcome resistances on their side and also on the side of health professionals. It is also necessary to pay attention to technical standardization and interoperability aspects of ICT (Codagnone 2009). Health care systems have to face the challenges created by new ways of working, empowered citizens and new tools.

The visional, collaborative, sustainable citizen-centered health environment offers means to gradually migrate from the current situation to a citizen-centered care environment. We are in good progress with PHS and PHR and also with health ICT infrastructures and next we need to give the citizen a participatory role in health care activities.

Acknowledgments We acknowledge the partial funding of this research by Academy of Finland through Trusted eHealth and eWelfare Space-project in the MOTIVE Research Programme 2009–2012.

References

Aaltonen, J., Ailio, A., Kilpikivi, P. et al. (2009). Kansallisen tason sähköisten potilastietojärjestelmien toteuttamisvaihtoehtojen vertailu – Kattava projekti. SITRAn selvityksiä 12, http://www.sitra.fi (in Finnish).

Adler-Milstein, J., Bates, D. W., & Jha, A. K. (2009). US regional health information organisations: Progress and challenges. *Health Affairs, 28*, 483–492.

AHIMA e-HIM Personal Health Record Work Group. (2005). Defining the personal health record. *Journal of AHIMA, 76*(6), 24–25.

Ash, J. S., & Bates, D. W. (2005). Factors and forces affecting EHR system adoption: Report of a 2004 ACMI discussion. *Journal of the American Medical Informatics Association, 12*, 8–12.

Basch, P. (2005). Electronic health records and the national health information network: Affordable, adoptable and ready fro prime time? *Annals of Internal Medicine, 143*, 227–228.

Berry, L. L., & Mirabito, A. M. (2010). Innovative healthcare delivery. *Business Horizons, 53*, 157–169.

Boulos, M. N. K., & Wheeler, S. (2007). The emerging Web 2.0 Social software: An enabling suite of sociable technologies in health and health care education. *Health Information and Libraries Journal, 24*(1), 2–23.

Center for Information Technology Leadership (CITL). (2008). The value of personal health records. *Healthcare Information and Management Systems Society (HIMSS)*, http://www.citl.org/publications/_pdf/CITL_PHR_Report.pdf. Accessed 28 Aug 2010.

Clarke, J. L., & Meiris, D. C. (2006). Electronic personal health records come of age. *American Journal of Medical Quality, 21*(3 Suppl), 5S-15S.

Codagnone, C. (2009). *Reconstructing the whole: Present and future of personal health systems*, PHS2020, European Commission, http://ec.europa.eu/information_society/activities/health/docs/projects/phs2020/phs2020-book-rev16082009.pdf. Accessed 28 Aug 2010.

Connecting for Health. (2008). *Common framework for networked personal health information: Consumers as network participants*. Markle Foundation, http://www.connectingforhealth.org/phti/docs/ConsumerNetwork.pdf. Accessed 28 Aug 2010.

Continua Health Alliance. (2005). Connected Personal Health in 2015: "Getting it Right!" – Looking back on the emergence of integrated person-centered health. Continua Health Alliance, http://www.continuaalliance.org/static/cms_workspace/CHA_WP081408v07.pdf. Accessed 28 Aug 2010.

De la Fuente, M. W., & Ros, L. (2009). A health collaborative network focus on self care processes in a personal assistant. *IFIP Advances in ICT, 307*, 759–766.

Detmer, D., & Steen, E. (2006). *Learning from abroad: Lessons and questions on personal health records for national policy*. The American Association of Retired Persons (AARP), http://assets.aarp.org/rgcenter/health/2006_10_phr_abroad.pdf. Accessed 28 Aug 2010.

Detmer, D., Bloomrosen, M., Raymond, B., & Paul, T. C. (2008). Integrated personal health records: Transformative tools for consumer-centric care. *BMC Medical Informatics and Decision Making, 8*:45, http://www.biomedcentral.com/1472-6947/8/45/. Accessed 28 Aug 2010.

eHealth roadmap – Finland. (2007). Reports of the Ministry for Social Affairs and Health, 2007:15, Helsinki.

European Commission, DG Information Society and Media, eHealth Unit (2006), Research Book of EU projects on Health. Brussels.

Fayn, J., & Rubel, P. (2010). Toward a personal health society in cardiology. *IEEE Transactions on Information Technology in Biomedicine, 14*(2), 401–9.

Frantzidis, C. A., & Bamidis, P. D. (2009). Description and future trends of ICT solutions offered towards independent living: The case of LLM project. *ACM international conference proceeding series. Proceedings of the 2nd international conference on pervasive technologies related to assistive environments*. Corfu, Greece (PETRA 09), ACM, New York, USA.

Froomkin, M. A. (2008). *The new health information architecture: Coping with the privacy implications of the personal health records revolution*. UM ELSI Group for Project HealthDesign.

Ganesh, J. (2004). E-health – drivers, applications, challenges ahead and strategies: A conceptual framework. *Indian Journal of Medical Informatics, 1*, 39–47.

Halamka, J. D., Mandl, K. D., & Tang, P. C. (2008). Early experiences with personal health records. *Journal of the American Medical Informatics Association, 15*, 1–7.

Halonen, R. (2010). Social media as a means of peer support. In R. Suomi & I. Ilveskoski (Eds.), *Navigating the fragmented innovation landscape*. *Proceedings of the 3rd international conference on well-being in the information society (WIS2010)*, Turku, Finland (pp. 48–60). TUCS General Publication 56, August, Turku, Finland.

Hawn, C. (2009). Report from the field: Take two aspirins and tweet me in the morning: How twitter, facebook and other social media are reshaping health care. *Health Affairs, 28*(2), 361–368.

Hill, J. W., & Powell, P. (2009). The national healthcare crisis: Is eHealth a key solution? *Business Horizons, 52*, 265–277.

Iliakovidis, I., Wilson, P., and Healy, J. C. (Eds.) (2005). *eHealth. Current situation and examples of implemented and beneficial ehealth applications*. The Netherlands: IOS Press.

James, G. A. (2007). Social, ethical and legal barriers to eHealth. *International Journal of Medical Informatics, 76*(5-6), 480–3.

Jha, A. K., Doolan, D., Grandt, D., Scott, T., & Bates, D. W. (2008). The use of health information technology in seven nations. *International Journal of Medical Informatics, 77*(12), 848–854.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! the challenges and opportunities of social media. *Business Horizons, 53*, 59–68.

Kolitsi, Z., & Cabrera, M. F. (2007). *Personal health systems: Deployment opportunities and ICT research challenges – Conference report*. February 12–13, 2007, Brussels. European Commission http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=323. Accessed 28 Aug 2010.

Koop, C. E., Mosher, R., Kun, L., Geiling, J., Grigg, E., Long, S., Macedonia, C., Merrell, R., Satava, R., & Rosen, J. (2008). Future delivery of health care: Cybercare. *IEEE Engineering in Medicine and Biology Magazine, 27*(6), 29–38. November-December.

Lee, H. J., Lee, S. H., Ha, K. S., Jang, H. C., Chung, W. Y., Kim, J. Y., Chang, Y. S., & Yoo, D. H. (2009). Ubiquitous healthcare service using Zigbee and mobile phone for elderly patients. *International Journal of Medical Informatics, 78*(3), 193–8.

Lopez, K. (2007). Global perspective on PHRs: Consumer engagement in health information exchange in Europe & the U.S., presentation, http://www.nocalhimss.org/events/presentations/ICW-Presentation.ppt. Accessed 28 Aug 2010.

Lorenzi, N., Kouroubali, A., Detmer, D., Bloomrosen, M. (2009). How to successfully select and implement electronic health records (EHR) in small ambulatory practice settings. *BMC Medical Informatics and Decision Making 9*: 15, http://www.biomedcentral.com/1472-6947/9/15. Accessed 28 Aug 2010.

Maglaveras, N., Chouvarda, I., Koutkias, V. G., Gogou, G., Lekka, I., Goulis, D., Avramidis, A., Karvounis, C., Louridas, G., & Balas, E. A. (2005). The citizen health system (CHS): A modular medical contact center providing quality telemedicine services. *IEEE Transactions on Information Technology in Biomedicine, 9*(3), 353–62.

Malmqvist, G., Nerander, K. G., & Larsson, M. (2005). Sjunet – The national IT infrastructure for healthcare in Sweden. In: I. Iliakovidis, P. Wilson, & J. C. Healy (Eds.), *Current situation and examples of implemented and beneficial eHealth application*, (pp. 41–49). The Netherlands: IOS Press.

Markle Foundation. (2003). Connecting for health: The personal health working group final report, July 1, http://www.connectingforhealth.org/resources/final_phwg_report1.pdf. Accessed 28 Aug 2010.

Mattila, E., Korhonen, I., Merilahti, J., Nummela, A., Myllymaki, M., & Rusko, H. (2008). A concept for personal wellness management based on activity monitoring. *Second international conference on pervasive computing technologies for healthcare, PervasiveHealth 2008*, pp. 32–36, Jan. 30, 2008–Feb. 1, 2008, Tampere, Finland.

Mattila, E., Korhonen, I., Salminen, J. H., Ahtinen, A., Koskinen, E., Sarela, A., Parkka, J., & Lappalainen, R. (2010). Empowering citizens for well-being and chronic disease management with wellness diary. *IEEE Transactions on Information Technology in Biomedicine, 14*(2), 456–463.

McConnell, H. (2004). International effort in implementing national health information infrastructure and electronic health records. *World Hospitals and Health Services, 40*(1), 33–52.

Monteagudo, J. L., & Moreno, O. (2007). D2.5, Report on Priority Topic Cluster two: Patient Empowerment. eHealth ERA (http://www.ehealth-era.org/documents/eH-ERA_D2.5_Patient_Empowerment_Final_31-03-2007_revised.pdf). Accessed 28 Aug 2010.

National Committee on Vital and Health Statistics (NCVHS). (2006). Personal Health Records and Personal Health Record Systems, U.S. Department of Health and Human Services, Feb. 2006.

Nykänen, P. (2008). Requirements for user friendly personal ehealth information systems. *International council for medical and care compunetics (ICMCC) conference*, June 2008, London, UK. In: L Bos, B Blobel, A Marsh and D Carroll (Eds.), Medical care and compunetics. Studies in Technology and Informatics 137. IOS Press, Amsterdam, 367–372.

Nykänen, P., Ruotsalainen, P., Blobel, B., & Seppälä, A. (2009). Research on trusted personal health and wellness information in ubiquitous health information space. In D. Dössel & W. C. Schlegel (Eds.), *World congress on medical physics and biomedical engineering, Munchen, Germany.. IFMBE Proceedings 25/XII* (pp. 432–435). Berlin: Springer.

Ohashi, M., Hori, M., & Suzuki, S. (2010). Citizen-centric e-healthcare management based on pervasive authentication – New ICT roadmap to active ageing. *Fourth international conference on pervasive computing technologies for healthcare (PervasiveHealth)*, Munich, Germany.

Osmani, V., Balasubramaniama, S., & Botvich, D. (2008). Human activity recognition in pervasive health-care: Supporting efficient remote collaboration. *Journal of Network and Computer Applications, 31*(4), 628–655. November.

Pagliari, C., Detmer, D., & Singleton, P. (2007). *Electronic personal records: Emergence and implications for the UK*. The Nuffield Trust, http://www.nuffieldtrust.org.uk/ecomm/files/Elec%20Personal%20Records%20II.pdf. Accessed 28 Aug 2010.

Pratt, W., Unruh, K., Civan, A., & Skeels, M. (2006). Personal health information management. *Communication of the ACM, 49*(1), 51–55.

Prentza, A., Maglavera, S., & Maglaveras, N. (2006). Quality healthcare management and well-being through INTERLIFE services: New processes and business models. *D2H2 1st transdisciplinary conference on distributed diagnosis and home healthcare* (pp. 109–112), 2–4 April 2006, Arlington, USA.

PricewaterhouseCoopers Health Research Institute. (2005). *Healthcast 2020: Creating a sustainable future. Pricewaterhousecoopers*, http://www.pwc.com/us/en/healthcast/past-reports.jhtml. Accessed 28 Aug 2010.

Pulli, P., Metso, A., & Zheng, X. (2008). *Ubiquitous services for senior citizens – service architecture and middleware*. Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL '08. First International Symposium on , vol., no., pp.1–5, 25–28 Oct. 2008, Aalborg, Denmark.

Quinn, C. C., Gruber-Baldini, A. L., Shardell, M., Weed, K., Clough, S. S., Peeples, M., Terrin, M., Bronich-Hall, L., Barr, E., & Lender, D. (2009). Mobile diabetes intervention study: Testing a personalized treatment/behavioral communication intervention for blood glucose control. *Contemporary Clinical Trials, 30*(4), 334–346. 1 July.

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association, 13*, 121–126.

Tang, P. C., & Lansky, D. (2005). The missing link: Bridging the patient — Provider health information gap. *Health Affairs, 24*(5), 1290–1295. Sep/Oct.

Teperi, J., Porter, M. E., Vuorenkoski, L., & Baron, J. (2009). *The Finnish health care system: A value-based perspective*. Sitra Reports 82, http://www.sitra.fi Accessed 28 Aug 2010.

The Long Lasting Memories. (2010), http://www.longlastingmemories.eu/. Accessed 23 Aug 2010.

Varshney, U. (2007). Pervasive healthcare and wireless health monitoring. *Mobile Networks and Applications, 12*, 113–127.

Wartena, F., Muskens, J., & Schmitt, L. (2009). Continua: The impact of a personal telehealth ecosystem. *International conference on eHealth, telemedicine, and social medicine, eTELEMED '09*, Cancun, Mexico.

World Health Organization (WHO). (2006). *Gaining health – The European strategy for the prevention and control of noncommunicable diseases*. Copenhagen, Denmark: WHO, Regional Office for Europe.

Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 596749, 10 pages
doi:10.1155/2012/596749

Research Article

Development of Personal Wellness Information Model for Pervasive Healthcare

Antto Seppälä,[1] Pirkko Nykänen,[1] and Pekka Ruotsalainen[2]

[1] *eHealth Research Group, School of Information Sciences, University of Tampere, P.O. BOX 607, 33014 University of Tampere, Finland*
[2] *Department of Information, National Institute for Health and Welfare, P.O. Box 30, 00271 Helsinki, Finland*

Correspondence should be addressed to Antto Seppälä, antto.seppala@uta.fi

Received 2 March 2012; Accepted 8 August 2012

Academic Editor: Rui Zhang

Pervasive healthcare and citizen-centered care paradigm are moving the healthcare outside the hospital environment. Healthcare delivery is becoming more personalized and decentralized, focusing on prevention and proactive services with a complete view of health and wellbeing. The concept of wellness has been used to describe this holistic view of health, which focuses on physical, social, and mental well-being. Pervasive computing makes it possible to collect information and offer services anytime and anywhere. To support pervasive healthcare with wellness approaches, semantic interoperability is needed between all actors and information sources in the ecosystem. This study focuses on the domain of personal wellness and analyzes related concepts, relationships, and environments. As a result of this study, we have created an information model that focuses on the citizens' perspectives and conceptualizations of personal wellness. The model has been created based on empirical research conducted with focus groups.

1. Introduction

Healthcare delivery is undergoing a notable shift toward personalized services with distributed care processes that emphasize a more holistic view of health and wellness within a citizen-centered care model [1–6]. The new citizen-centered care paradigm focuses on the health, functioning, and well-being of people as a whole [7]. The focus, then, is more on preventive, proactive services with the citizen at the core of his/her care, instead of just treating diseases and symptoms [1, 2, 4–6]. In the future, it will not be enough to just access medical histories or test results, but citizens' lifestyle information, behavioral choices, and monitoring and measurement data will need to be considered to ensure preventive, proactive service [2, 4–6].

Such a view of health is not entirely new. The World Health Organization (WHO) defined health as early as 1948 as "a state of complete physical, mental and social well-being and not merely the absence of disease of infirmity" [8, page 100]. This definition acknowledged a holistic view of health and supported a focus beyond disease treatment. Despite this WHO's definition, the concept of health may cause misunderstandings because usually it is understood to refer to a person's state when free of diseases, and the focus is on medical well-being. However, health can be defined in many ways, for example, it can be seen as a state of stable physiological function, lack of diseases, and absence of illnesses. One term that has been used to describe more complete health and well-being of people is wellness. Wellness is thought to be a subjective feeling of health and well-being [9]. Wellness considers individuals' general functioning as a whole, covering not only physical but also social and psychological aspects [9, 10]. Wellness is a multidimensional concept, and it is currently being studied in many different scientific areas, such as medicine, public health, occupational health, and mental health [9].

2. Research Context and Objectives

Pervasive healthcare can be defined either as the application of pervasive computing—in other words, ubiquitous computing, proactive computing, or ambient intelligence—for healthcare, health, and wellness management, or as making healthcare available anytime and anywhere [11].

The basic idea behind pervasive healthcare is to integrate healthcare technologies and concepts into people's everyday lives. Pervasive healthcare is seen as supporting the shift toward citizen-centered care [12, 13]. Very closely related to pervasive healthcare is the research being done in the pervasive and ubiquitous computing fields. These technology paradigms focus on embedded, mobile, proactive, context-aware, collaborative, and sensor systems [13].

Pervasive healthcare applications are designed to support decentralized and preventive care. Pervasive healthcare will also help citizens manage their personal health and wellness outside the provider network. This model highlights a wellness-centered approach by helping citizens to stay well physically, mentally, and socially and to utilize different self-management and assistive services [13]. With pervasive computing technologies, it is it possible to collect all kinds of data anytime and anywhere [11, 14]. Data collection can be done by using intelligent sensors and measurement technologies.

The objective of information modeling is to describe the information in a certain domain or in an organization. Information models can be used to capture users' perceptions and understanding of system complexities [15]. In this study, we are focusing on the conceptual level of modeling. Conceptual modeling takes as its point of interest knowledge about the domain, and the idea is to build a representation of the real-world semantics [16, 17]. Conceptual modeling can be performed using informal or semiformal models. Despite of the formality level of used modeling notation, the main aim is to capture concepts and relationships in the target domain [18, 19].

With pervasive healthcare and more personalized, holistic, and citizen-centered services, we need a better understanding of the personal wellness domain. This requires more information than typical health records include. To fully support the new ways of managing health and wellness with ICT and pervasive computing, we need to achieve semantic interoperability among different stakeholders, systems, devices, sensors, and other information sources and users. To achieve semantic interoperability, a context-aware personal wellness ontology is needed. This ontology can be used to create shared understandings and allow for sharing of heterogeneous information among all actors and systems in the personal wellness ecosystem.

This study is a part of a research project that examines the trusted use of personal health and wellness information in future ubiquitous computing environments [20]. In this research project, we aim to create a trusted context-aware ontology for lifelong personal wellness management and an architecture model for trusted use of multisource heterogeneous information. Before we can start building a personal wellness ontology, we have to understand what wellness is, what its components are, what information is related to it, how people manage and maintain wellness, and what influences wellness. Basically, we have to uncover the scope and contents of the concept of wellness. This study develops the wellness concept further and builds the basis for the development of a personal wellness ontology.

The first research objective of this study was to analyze the domain of personal wellness. This includes both how the concept of personal wellness is defined in the literature and how people conceptualize it as well as the scope of the domain. The second objective of this study was to create a high-level personal wellness information model to present related concepts, characteristics, and contextual aspects. With this high-level information model, we can understand the concept of personal wellness and start to create a more formal model, in other words, a personal wellness ontology.

3. Methods

As a guiding framework for our research, we have used a design science research (DSR) approach [21, 22]. DSR can be seen as a problem-solving process in which actual business needs are addressed by building actual artifacts or applications. DSR is usually considered to address particularly problematic situations that are characterized by unstable requirements and constraints, complex interactions, a tendency to change in terms of design processes or artifacts, and dependence upon human cognitive and social abilities [22].

DSR is based on two design processes: *build* and *evaluate*. These two processes produce IT artifacts, which can be constructs, models, methods, or implementations. Usually build and evaluate processes are performed iteratively to improve the quality of the artifact. Hevner et al. [22] have developed seven guidelines for DSR, and we have followed these during our research. These guidelines are (a) design as an artifact, (b) problem relevance, (c) design evaluation, (d) research contribution, (e) research rigor, (f) design as a search process, and (g) communication of research. In this study, we focus on building and evaluating both the constructs and a model in the personal wellness domain. The constructs define the basic concepts, the universe of discourse, and the relations and attributes of the concepts.

Most of the work done in the domain of personal wellness is related to the measurement or assessment of wellness or well-being. They focus on different things than what we need to develop a personal wellness ontology. These models are high-level descriptions with limited analysis of the concepts or relations. Moreover, environmental factors are defined quite narrowly. In our research, we are more interested in identifying and defining main components, concepts, and relations in the personal wellness domain. We are creating a more complete and conceptually focused model to support the field of pervasive healthcare.

This study had three main methods for information modeling:

(1) an analysis of the literature, which explores the conceptualization of personal wellness, personalized healthcare, and a holistic view of health;

(2) a context analysis to identify internal and external contexts of personal wellness;

(3) focus groups to understand how people understand the concept of personal wellness, how it can be conceptualized, and which factors affect personal wellness.

Table 1: Focus group meetings.

Group	Duration	Participants	Focus
Group 1	2 meetings, 4 hours each	Young, healthy department staff members, open voluntary call to our department's mailing list (5 and 4 participants)	Identify and describe basic concepts of personal wellness
Group 2	1 meeting, 2 hours	Internal project meeting (4 participants)	Specification of concepts, redundancy reduction, and abstraction levels
Group 3	1 meeting, 2 hours	Our university's health informatics postgraduate students (5 participants)	Concept specification and categorization and external contexts
Group 4	2 meetings, 2 hours each	Females aged 48–62 (9 and 10 participants); group was formed on a voluntary basis by sending invitations to participants in another well-being-related study	Discussion about participants' views on personal wellness in general and then our models in more detail

3.1. Literature Analysis. As a basis for the study, we carried out an analysis of scientific literature concerning personal wellness. The analysis included Google Scholar and different scientific publication databases: Association for Computing Machinery (ACM), ESBCOhost Academic Search Premier, IEEE, PubMed, ScienceDirect, and SpringerLink. For more detailed analysis, we chose articles concerning holistic and multidimensional views on health and wellness that possibly were related to the components of a citizen-centered healthcare paradigm. We manually analyzed around 100 articles concerning these topics.

3.2. Context Analysis. The context analysis was performed using basic techniques from the requirements elicitation process. Requirements elicitation is a process used to find necessary requirements for computer-based systems [23]. In our case, the target was the existing knowledge in the literature. We analyzed the application domain, identified the source documents related to our domain, and recognized and analyzed related stakeholders. The stakeholders, in our case, were the internal and external contexts in personal wellness. We identified both external environment and internal environment, the latter of which consists of factors related directly to the person herself, such as things that she herself can affect, control, influence, or manage.

3.3. Empirical Studies with Focus Groups. From the literature and context analysis, we obtained the material that formed the basis of our empirical research, which was performed with focus groups. A focus group is a method for group interviews in which emphasis is on the communication between the participants. The number of groups or participants may vary, but according to Kitzinger [24], the ideal number of participants in the group is from four to eight. The idea is to generate data based on interaction and communication, instead of the researcher asking the participants direct questions. Focus groups are a useful method for exploring knowledge and experiences of people because they can help people explain and clarify their thoughts and views. It is especially suitable for situations in which the existing knowledge is inadequate, the subject is very complex with many variables, and the research questions are very open. Sometimes, though, the group dynamics might silence some participants or ideas. Methods for conducting focus group-centered research may vary, depending on several factors, such as the number of participants or groups, how the groups are formed (preexisting or unknown), and the homogeneity or heterogeneity of the participants [24, 25].

The total number of focus group meetings in our study was six, with four different groups (see Table 1). The focus group meetings were organized such that one of the researchers acted as a head of the meetings and the researchers collected the results based on the discussions. To support the meetings, we had some themes and models, but the structure of the focus groups meetings was quite relaxed and informal, and the participants were encouraged to discuss their views openly. The objective of the focus groups was to gather empirical material about how personal wellness is understood and conceptualized and what kinds of contexts are related to it. This meant that it was important to collect concepts and the ideas behind them that were revealed during the groups' communication.

The results of the first two meetings were documented in a mind map. Mind mapping was chosen because it is an easy way to represent information, simple categorizations, and simple relations between concepts. Moreover, most people are familiar with this technique. Based on the first two focus group meetings and the performed analyses, we started to model the personal wellness domain in a more formal way by using a simplified entity relationship (ER) notation. The idea behind the use of the simplified ER model was that the model could be easily understood and modified by people without any modeling experience. The results and modifications made by the focus group participants were modeled by the researchers. Although we performed the modeling ourselves based on the focus group meetings, we tried, to the extent possible, to keep the model based on the actual discussions, concepts, and views presented by the focus group participants. The modeling work was divided into seven sub-models, which together form the high-level information model of personal wellness. The focus group meetings were organized to support iterative build-evaluate-type process.

4. Results

4.1. Conceptualizing Personal Wellness: Results from the Literature and Context Analysis. Wellness is a multidimensional and multidisciplinary concept. Although definitions may vary depending on the context, generally, wellness is thought to be a balanced state of a healthy body, mind, and

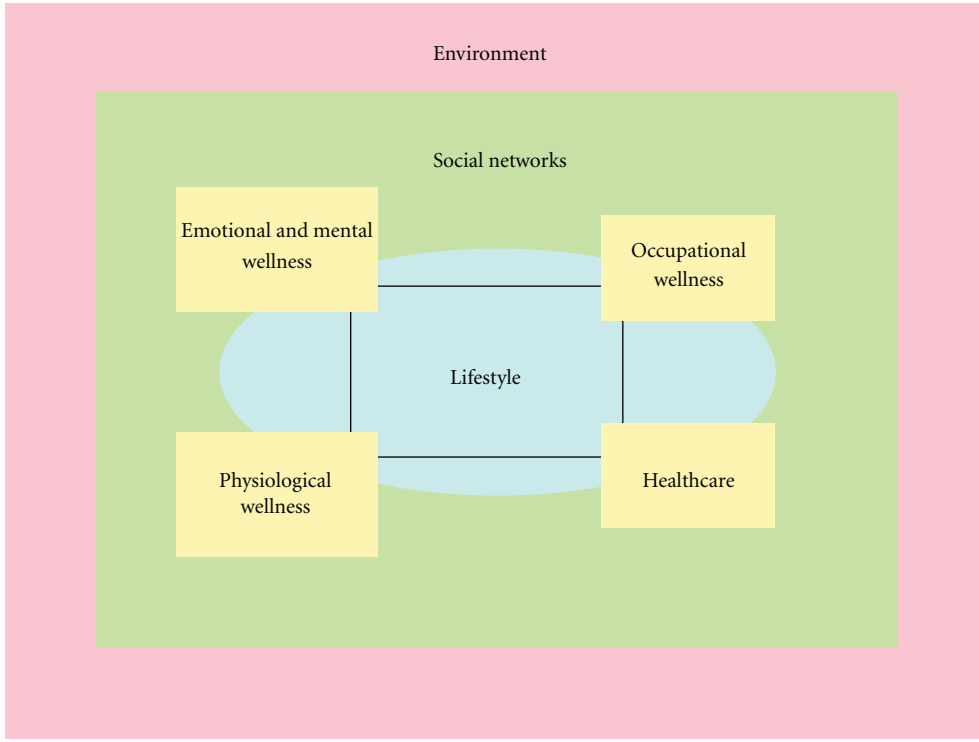


Figure 1: Personal wellness domain.

spirit [7, 9, 10, 26–28]. Wellness can be seen as a high-level concept that integrates multiple domains, including the physical, psychological, social, and spiritual domains, and it may vary according to age or cultural context [29]. Also, health promotion, prevention, and better functioning are closely related to wellness [7, 27, 30, 31]. Wellness is a complete, holistic view that focuses on the individual and his specific needs. It takes into account the whole person and her environment, acknowledging lifestyle, behavior, culture, beliefs, experiences, and other aspects that affect a person's life [9, 10, 27, 31–33].

Some holistic wellness models have been developed in the field of clinical and counseling psychology [34]: the Wheel of Wellness by Sweeney and Witmer [35], the Indivisible Self by Myers and Sweeney [26], the Circle of Health by Saylor [36], and an ecosystemic approach to health, well-being, and wellness by Kirsten et al. [28]. All four models take a holistic, multidimensional view of health and wellness. The models were quite high-level, informal, and general, and their purpose was different from ours, but we were able to extract some of their concepts and other characteristics. For more information about these models and analyses, see [37].

Based on the literature and context analyses, we were able to identify some common concepts, characteristics, and properties of personal wellness. As a result of the analyses, we were able to discover how wellness is defined as a high-level concept, as well as the common characteristics and components wellness is generally thought to have [37]:

(i) It is a holistic, multidimensional, and multidisciplinary view of health and well-being;

(ii) Wellness is a broader concept than most views on health as defined by healthcare; it takes into account environmental, emotional, intellectual, occupational, social, and spiritual aspects of well-being;

(iii) It focuses on complete health and well-being, prevention, and proactive services;

(iv) It is dynamic and context-dependent.

4.2. Empirical Refinement of the Personal Wellness Concept. Based on the literature and context analyses and the first two focus group meetings, we created our own view of personal wellness (Figure 1). The view of personal wellness consists of five internal components and two external contexts. The internal components are: lifestyle, emotional and mental wellness, occupational wellness, healthcare, and physiological wellness. The two external contexts are: social networks and environment. In our view, all components are linked together, which represents the complete and holistic nature of personal wellness in which there are many different relationships between components. This view emphasizes the notion that personal wellness is much more than just physical health and well-being. In this light, it is clear that it should be examined in a multidisciplinary and multi-professional context.

The lifestyle component is a kind of background component that directly affects the other four internal components. The lifestyle component includes concepts regarding activities, behaviors, choices, and risk factors related to person's lifestyle. Emotional and mental wellness focuses on concepts concerning individual identity, psychological concepts, intellectual wellness, emotions, feelings, and so

forth. Emotional and mental wellness also includes a person's views and values that affect choices and behaviors.

Occupational wellness is about well-being related to people's occupations, and in this context, occupation can mean that the person is working, studying, unemployed, retired, or an entrepreneur. Occupational wellness considers the actual occupation and its effects on personal wellness. Physiological wellness focuses on information related to health and wellness that is not bound to certain healthcare provider, for example, conditions, disabilities, functioning, genetics, monitoring and measuring data, personal observations, and so forth. The healthcare component is about the healthcare system. It includes providers, medical documents, and services.

All of these internal components of personal wellness are surrounded and affected by external contexts—social networks and environment. Social networks include all social relations that affect a person. Environment describes the digital and physical environments related to the person in question. It includes, for example, living environment, service environment, society, cultural aspects, and regulations. The environment surrounding a person is very dynamic, flexible, and sensitive, and it may change over the course of a lifetime.

From the first two focus group meetings alone, we already had quite a lot of different concepts related to personal wellness. We had gathered these concepts into two mind maps, so we had some categorization and simple relations between these concepts. From these mind maps, we started to categorize concepts into models, loosely based on the simplified ER diagram. We created seven different models to represent all the components of personal wellness. In these models, we focused more on the concepts and their categorization because these are core components of ontology development.

We started going through these models with the different focus groups to get a more detailed view and to discover the necessary concepts related to personal wellness. In the focus group meetings, the participants were encouraged to openly discuss current themes. Between the focus group meetings, we analyzed the discussions and the feedback for the meetings and based on this, we revised the models, analyzed and added new concepts into the models, reduced redundant concepts, and considered different relationships between concepts. The resulting high-level personal wellness information model will be introduced in more detail in the next section.

4.3. Personal Wellness Information Model. As a result of the combination of all three methods, we were able to create an information model that describes our view of personal wellness. The lifestyle component describes the domain of personal lifestyle and consists of activities, behaviors, and choices that affect the person's daily life. It also includes active wellness activities and management concepts. These concepts are such that they can usually be affected, controlled, influenced, or managed by the person herself. Lifestyle focuses on concepts that are quite dependent on the person herself, and their emphasis may vary a lot between people. Listed below are the main concepts and subconcepts of lifestyle:

(i) livelihood;

(ii) nutrition—experiences, history, food diaries, diet;

(iii) rest/relaxation, sleep;

(iv) risk factors—behavioral, environmental, inheritable;

(v) sexual behavior;

(vi) wellness activities—objectives, self-development, wellness maintenance (personal responsibility, active actions; self-evaluation), hobbies, leisure, fitness/exercise;

(vii) Wellness behavior—wellness management (activity management, alternative medicine, behavior management, conditions, devices, medication, nonprescribed medication), health education, prevention.

The emotional and mental component focuses on elements related to people's minds, feelings, emotions, identities, and personalities (Figure 2). The concepts in emotional and mental wellness describe personal views, feelings, and attitudes towards life, personality, and experiences. They also include mental health and possible disorders. This component is aimed at describing what is going on in the person's mind, how he will react to different situations, and how he can cope mentally. In the emotional and mental component, we used the categorization of Emotion Annotation and Representation Language (EARL) [38] to describe the emotions of a person.

Occupational wellness describes well-being related to person's occupation. A person's occupation can be, for example, work, studying, or being unemployed or retired. The concept of occupation describes the actual occupation, its properties, or how the person feels about it. It has some subconcepts, which include: appreciation, benefits, equality, functioning, meaningful, motivation, performance, responsibilities, respect, rewarding, rights, and type. Occupational wellness includes also following concepts: education, employer, environment, income, occupational safety and health, quality of working life, social relations, vacation, volunteering, work burden, work climate, work culture (including leadership and management), working ability, and working time.

Physiological wellness has to do with health and wellness-related information outside the healthcare provider network. It will help the citizen to collect, observe, and manage her personal health information. It will include different health and wellness devices and their monitoring and measuring of data as well as information about a person's conditions and functioning. Physiological wellness is closely related to the concept of the personal health record, but the idea is to be more thorough and complete through an emphasis on information and events outside the healthcare provider network. It includes the following concepts: conditions, demographic information, disability, functioning, genetic information, measurement and monitoring data, observation, organ system, vital signs, and wellness devices.

The healthcare component focuses on the clinical side of wellness. It has to do with the regulated healthcare system

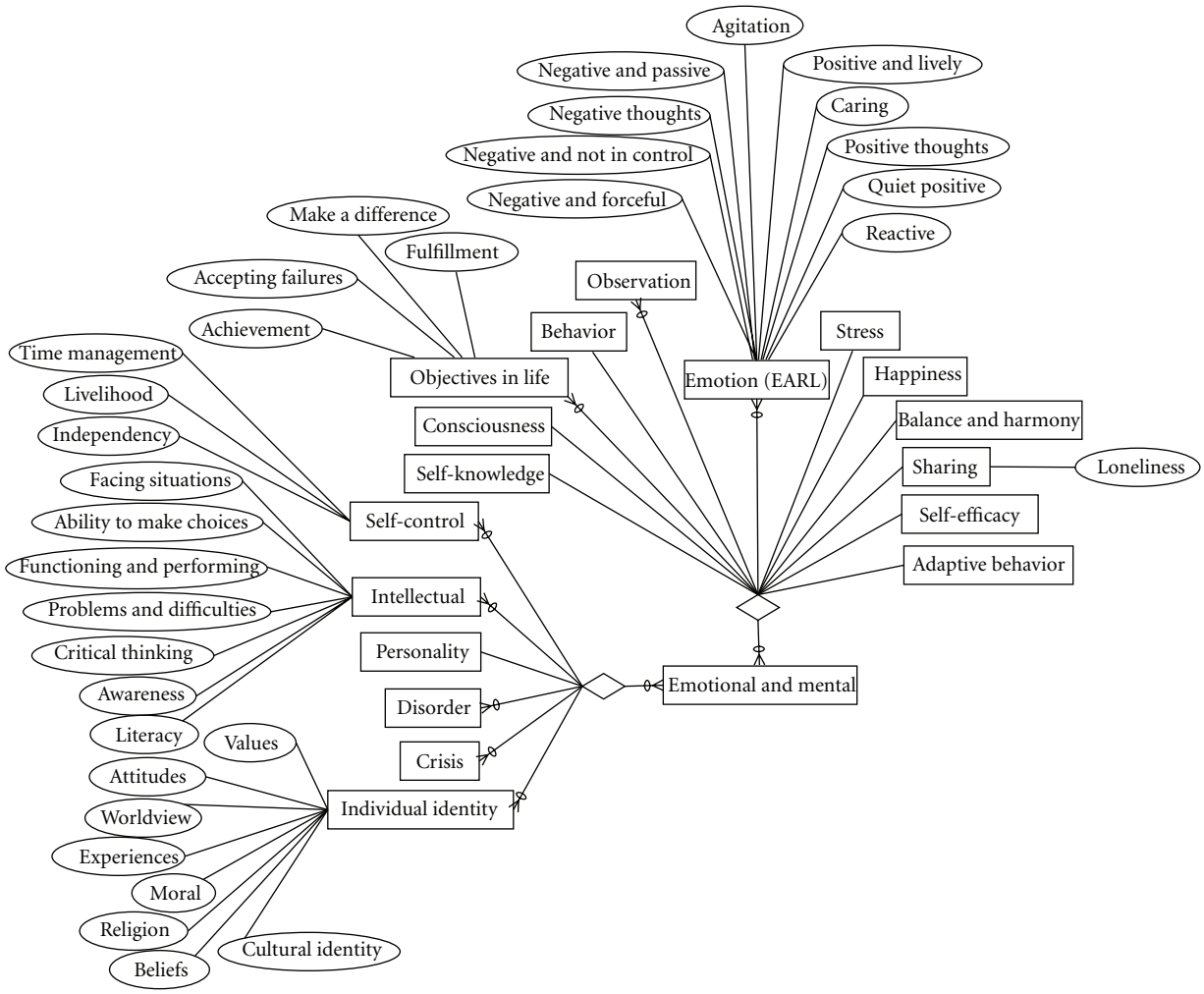


Figure 2: Emotional and mental wellness.

and the actual care that the person receives. The model consists of two main concepts: service and provider. The service concept is divided into three subconcepts, or types: prevention, diagnosis, and treatment. All of these different services create medical documents, and from these documents, the medical history of a person is created. Providers are divided into four subconcepts, or types: preventive, curative, promotional, and rehabilitative.

The social networks component describes the different social relations and networks that are related to a person. It includes family, relatives, and friends, but also different communities and social environments, and the social participation of a person within these contexts. Most of the external contexts that affect people's living and personal wellness are located in the environment component. This includes different kinds of environments, such as society, cultural norms, or the media (Figure 3). The environment affects the person in many ways, and it may shape the possibilities for handling personal wellness. These external factors are heavily context-dependent and may differ from country to country.

All seven components combined create a high-level information model of the personal wellness domain (Figure 4).

5. Discussion

As a result of this research, we were able to create a high-level information model of the personal wellness domain. Usually, health-related information models and ontologies are built from the healthcare systems and the service providers' viewpoint. Here, however, we have instead created our model from the citizens' viewpoint. The citizens' viewpoint is based on the empirical research performed with the focus groups. We tried to get a comprehensive view with participants from different age groups with different backgrounds but as the focus groups were created on a voluntary basis from a limited pool of people there can be some limitations in the model. Also the participants can be seen being more interested in their health and wellness than regular citizens as they are willing to participate in this kind of voluntary research. With focus groups we have created a model based on active

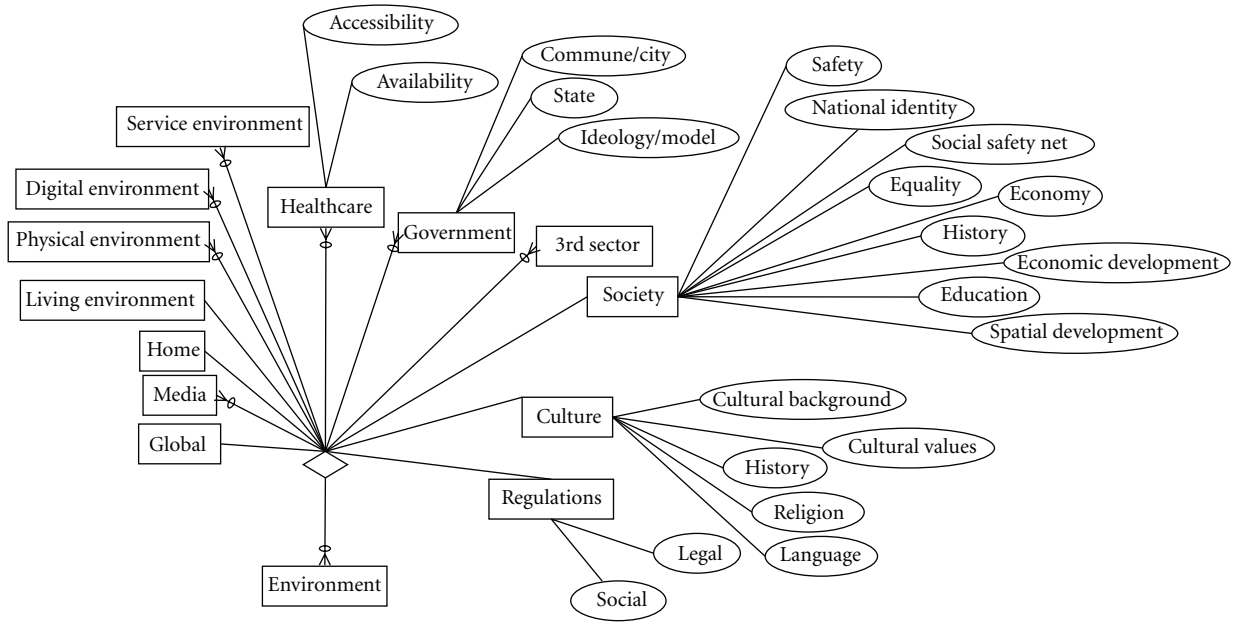


Figure 3: The environment component.

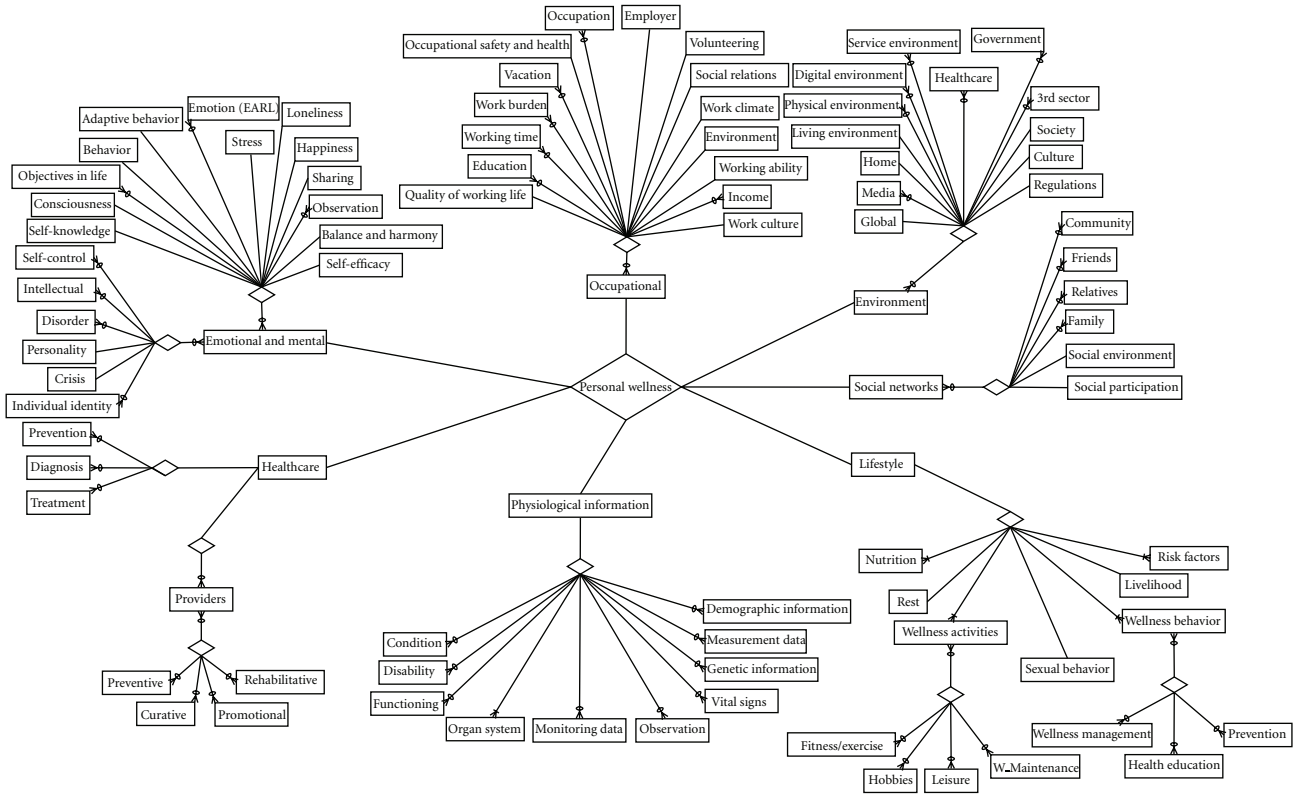


Figure 4: The highest level concepts of personal wellness.

and conscious people who are not health professionals or representatives of any health organizations.

The model is based on the focus group research, and we have tried to model the domain and the concepts according to the participants. The guiding principles of the modeling work were how citizens see their personal wellness, what they consider to be the important concepts, how they categorize these concepts, and how they understand the notion of complete, holistic health and wellness. The research process

was performed iteratively, following the build-evaluate idea of design science research.

We have identified the main components of personal wellness and described related information and its conceptualization. In the model, we have identified the environmental and external contexts related to personal wellness. In our model, we present many important concepts. Based on our categorization of these, we can come to understand the basic relations between concepts, and we can see some is-a relationships. There are still some limitations related to the defined concepts in terms of the development of the ontology, as some of the concepts are quite abstract, and their explicit definition can be challenging. Also, there is a great number of relations and relationship types in the domain, and most of the concepts are interconnected.

Hevner et al. [22] have defined seven guidelines that should be followed when performing design science research. The first guideline is to design as an artifact. In our research, we have built artifacts such as mind maps to describe common concepts—the constructs of the domain—and a high-level information model to describe the domain, how it is conceptualized, its scope, and some relationships. The second guideline is problem relevance, which means that the research problem should be relevant and solve some important problem in the constituent community. Pervasive healthcare and a more personalized, complete way of managing personal health and wellness are emerging, yet currently there is no real consensus regarding what personal wellness actually is or its components. Most of the research done on wellness has focused on the measurement or assessment of wellness. Also, the models related to wellness are high-level descriptions with limited conceptual definitions and relationships. Most of the information models and ontologies in the health domain are representations from the health service providers, clinical, or medical points of view. Our research brings new perspectives into the personal wellness domain by defining the citizens' perspective to support the development of a personal wellness ontology and semantic interoperability in the domain. Thus, our research problem is relevant in the personalized health and wellness domain.

The third guideline is about design evaluation. Hevner et al. [22] emphasized that the utility, quality, and efficacy of an artifact must be demonstrated by evaluation, which is a crucial part of the design process. Our design process was iterative, so we built and evaluated the model in various phases, but the evaluation of the model alone still insufficient. The study continues with an assessment phase, in which the developed model is evaluated with respect to its validity and potential impact on citizens' personal health and wellness. The model will be evaluated with use cases and usage scenarios. Design science research, according to the fourth guideline, should clearly contribute in at least one of the following ways: the design artifact, design construction knowledge, or design evaluation knowledge [22]. Our research makes a significant contribution by defining the personal wellness domain, how it is conceptualized, and what the necessary concepts and external factors are.

The fifth guideline emphasizes that the research should be conducted with rigorous methods. As the domain in question was complex, multidimensional, quite abstract, and based on citizens' perspectives, we began with qualitative methods, like focus groups and informal modeling methods. Although, the informal models lacked with formalism we were able to represent the complex and multidimensional domain and the models were rather easy for average citizens with no modeling experience to understand, evaluate, and modify. We had several different focus groups to get more heterogeneous views of personal wellness so that we could tackle the sixth guideline. This guideline emphasizes the importance of an iterative design process and insists that design should be a process of searching such that the design problem becomes more focused and the solution more relevant [22]. The next step in this study is the development of the ontology and context-aware architecture. Thus, the solution will be redefined in a process of searching. The seventh guideline is that the research should be communicated to technology and management audiences. This will be realized in later phases of the project.

6. Conclusions

In this research, we have approached complete, holistic health and well-being from the citizens' perspective. We have further refined the concept of personal wellness through empirical methods. Based on an analysis of the literature, a context analysis, and empirical research, we have created our own view of personal wellness. In order to support interoperable, citizen-centered services with upcoming pervasive wellness tools, we have identified the scope of the personal wellness domain. As a result of this research, we have developed a high-level information model that describes the main concepts and some relationships related to personal wellness. With this information model, we have started to develop a context-aware ontology. Our research brings new knowledge to the field of pervasive healthcare by identifying the citizens' perspectives and conceptualizations of personal wellness.

Our model describes the domain of personal wellness in more detail than other models that have been developed in clinical and counseling psychology. Such previous models remain general, while we have gone deeper into the personal wellness domain by defining more concepts, relationships, and properties. Moreover, the focus of our model is different from previous work, as we are addressing the problem from an information system science perspective, and we are using a different kind of representation style that is more suitable in our context. We are focusing on the pervasive healthcare field, and our intentions are to support the development of a personal wellness ontology for lifelong personal wellness management and an architecture model for trusted use of multisource heterogeneous information.

The next phases in our research are an assessment of our model and the development of the personal wellness ontology. The assessment phase focuses on the evaluation of the validity and utility of the model and the identification of the impact the shared use of wellness information has on citizens' wellness management and on how citizens can control and manage the use of their information. In the development of the personal wellness ontology, we have to model the

contextual aspects that are related to different concepts to support multiuser and multisystem environments with heterogeneous information sources. Furthermore, we have to consider privacy, confidentiality, and data security issues in the ontology, as most of the information is private and personal, and its processing may be regulated by legislation. By modeling such privacy and security aspects, we can ensure that, in the future, pervasive healthcare will allow citizens to control the processing of their information dynamically.

Acknowledgment

The authors acknowledge the funding of this Trusted eHealth and eWelfare Space (THEWS) research project by the Finnish Academy of Sciences in the MOTIVE Research Programme during 2009–2012.

References

[1] P. Nykänen, "Requirements for user friendly personal ehealth information systems," in *Studies in Health Technology and Informatics*, vol. 137, pp. 367–372, IOS Press, 2008.

[2] L. L. Berry and A. M. Mirabito, "Innovative healthcare delivery," *Business Horizons*, vol. 53, no. 2, pp. 157–169, 2010.

[3] C. Koop, R. Mosher, L. Kun et al., "Future delivery of health care: cybercare," *IEEE Engineering in Medicine and Biology Magazine*, vol. 27, no. 6, pp. 29–38, 2008.

[4] M. Ohashi, M. Hori, and S. Suzuki, "Citizen-centric e-healthcare management based on pervasive authentication-New ICT roadmap to active ageing," in *2010 4th International Conference on Pervasive Computing Technologies for Healthcare, Pervasive Health 2010*, pp. 1–8, March 2010.

[5] W. Pratt, K. Unruh, A. Civan, and M. Skeels, "Personal health information management," *Communications of the ACM*, vol. 49, no. 1, pp. 51–55, 2006.

[6] P. Nykänen and A. Seppälä, "Collaborative approach for sustainable citizen-centered health care," in *Critical Issues for the Development of Sustainable E-Health Solutions, Healthcare Delivery in the Information Age*, N. Wickramasinghe et al., Ed., pp. 115–134, Springer, New York, NY, USA, 2012.

[7] J. S. Larson, "The conceptualization of health," *Medical Care Research and Review*, vol. 56, no. 2, pp. 123–136, 1999.

[8] World Health Organization, *Preamble to the Constitution of the World Health Organization as Adopted by the International Health Conference*, World Health Organization, New York, NY, USA, 1948.

[9] S. Mackey, "Towards an ontological theory of wellness: a discussion of conceptual foundations and implications for nursing," *Nursing Philosophy*, vol. 10, no. 2, pp. 103–112, 2009.

[10] N. Oguz-Duran and E. Tezer, "Wellness and self-esteem among turkish university students," *International Journal for the Advancement of Counselling*, vol. 31, no. 1, pp. 32–44, 2009.

[11] I. Korhonen and J. E. Bardram, "Introduction to the special section on pervasive healthcare," *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 3, pp. 229–234, 2004.

[12] B. Arnrich, O. Mayora, J. Bardram, and G. Tröster, "Pervasive healthcare paving the way for a pervasive, user-centered and preventive healthcare model," *Methods of Information in Medicine*, vol. 49, no. 1, pp. 67–73, 2010.

[13] J. E. Bardram, "Pervasive healthcare as a scientific discipline," *Methods of Information in Medicine*, vol. 47, no. 3, pp. 178–185, 2008.

[14] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mobile Networks and Applications*, vol. 12, no. 2-3, pp. 113–127, 2007.

[15] K. Siau and Y. Wang, "Cognitive evaluation of information modeling methods," *Information and Software Technology*, vol. 49, no. 5, pp. 455–474, 2007.

[16] Y. Wand, D. E. Monarchi, J. Parsons, and C. C. Woo, "Theoretical foundations for conceptual modelling in information systems development," *Decision Support Systems*, vol. 15, no. 4, pp. 285–304, 1995.

[17] R. Weber, "Conceptual modelling and ontology: possibilities and pitfalls," *Journal of Database Management*, vol. 14, no. 3, pp. 1–20, 2003.

[18] H. S. Pinto and J. P. Martins, "Ontologies: how can they be built?" *Knowledge and Information Systems*, vol. 6, no. 4, pp. 441–464, 2004.

[19] H. S. Pinto and J. P. Martins, *Ontologies: How Can They Be Built?* Springer, New York, NY, USA, 2004.

[20] P. Nykänen, P. Ruotsalainen, B. Blobel, and A. Seppälä, "Research on trusted personal health and wellness information in ubiquitous health information space," in *Proceedings of the International Federation for Medical and Biological Engineering (IFMBE '09)*, pp. 432–435, September 2009.

[21] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decision Support Systems*, vol. 15, no. 4, pp. 251–266, 1995.

[22] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[23] D. Zowghi and C. Coulin, "Requirements elicitation: a survey of techniques, approaches, and tools," *Engineering and Managing Software Requirements*, pp. 19–46, 2005.

[24] J. Kitzinger, "Introducing focus groups," *BMJ*, vol. 311, no. 7000, pp. 299–302, 1995.

[25] R. A. Powell and H. M. Single, "Focus groups," *International Journal for Quality in Health Care*, vol. 8, no. 5, pp. 499–504, 1996.

[26] J. E. Myers and T. J. Sweeney, "The indivisible self: an evidence-based model of wellness," *Journal of Individual Psychology*, vol. 60, no. 3, pp. 234–245, 2004.

[27] C. Soomlek and L. Benedicenti, "Operational wellness model: a wellness model designed for an agent-based wellness visualization system," in *2nd International Conference on eHealth, Telemedicine, and Social Medicine (ETELEMED '10)*, pp. 45–50, February 2010.

[28] T. G. J. C. Kirsten, H. J. L. van der Walt, and C. T. Viljoen, "Health, well-being and wellness: an anthropological eco-systemic approach," *Health SA Gesondheid*, vol. 14, pp. 1–7, 2009.

[29] T. L. Schuster, M. Dobson, M. Jauregui, and R. H. I. Blanks, "Wellness lifestyles I: a theoretical framework linking wellness, health lifestyles, and complementary and alternative medicine," *Journal of Alternative and Complementary Medicine*, vol. 10, no. 2, pp. 349–356, 2004.

[30] P. Conrad, "Wellness as virtue: morality and the pursuit of health," *Culture, Medicine and Psychiatry*, vol. 18, no. 3, pp. 385–401, 1994.

[31] E. W. Sterling, S. A. Von Esenwein, S. Tucker, L. Fricks, and B. G. Druss, "Integrating wellness, recovery, and self-management for mental health consumers," *Community Mental Health Journal*, vol. 46, no. 2, pp. 130–138, 2010.

[32] R. A. Kiefer, "An integrative review of the concept of well-being," *Holistic Nursing Practice*, vol. 22, no. 5, pp. 244–252, 2008.

[33] A. Ahtinen, S. Ramiah, J. Blom, and M. Isomursu, "Design of mobile wellness applications: identifying cross-cultural factors," in *Proceedings of the 20th Australasian Conference on Computer-Human Interaction: Designing for Habitus and Habitat (OZCHI '08)*, pp. 164–173, December 2008.

[34] D. A. Els and R. P. De La Rey, "Developing a holistic wellness model," *SA Journal of Human Resource Management*, no. 2, pp. 46–56, 2006.

[35] T. Sweeney and J. M. Witmer, "Beyond social interest: striving toward optimum health and wellness," *Individual Psychology*, vol. 47, pp. 527–540, 1991.

[36] C. Saylor, "The circle of health: a health definition model," *Journal of Holistic Nursing*, vol. 22, no. 2, pp. 97–115, 2004.

[37] A. Seppälä and P. Nykänen, "Contextual analysis and modeling of personal wellness," in *Proceedings of the International Conference Knowledge Engineering and Ontology Development (KEOD '11)*, J. Filipe and J. L. G. Dietz, Eds., pp. 26–29, Paris, France, October 2011.

[38] HUMAINE Emotion Annotation and Representation Language (EARL): Proposalm, 2006, http://emotion-research.net/projects/humaine/earl/proposal.

Original Paper

A Conceptual Framework and Principles for Trusted Pervasive Health

Pekka Ruotsalainen[1], D.Sc (tech.); Bernd Blobel[2], PhD; Antto Seppälä[3], MSc; Hannu Sorvari[4], MSc; Pirkko Nykänen[3], PhD

[1]National Instutute for Health and Welfare, Department of Information, Helsinki, Finland

[2]University Hospital Regensburg, eHealth Competence Center, University of Regensburg, Regensburg, Germany

[3]School of Information Sciences, Centre for Information and Systems, University of Tampere, Tampere, Finland

[4]University of Turku, Faculty of law, Turku, Finland

Corresponding Author:
Pekka Ruotsalainen, D.Sc (tech.)
National Instutute for Health and Welfare
Department of Information
PL 30
Helsinki, 00271
Finland
Phone: 358 0505004046
Fax: 358 206102443
Email: pekka.ruotsalainen@thl.fi

Abstract

Background: Ubiquitous computing technology, sensor networks, wireless communication and the latest developments of the Internet have enabled the rise of a new concept—pervasive health—which takes place in an open, unsecure, and highly dynamic environment (ie, in the information space). To be successful, pervasive health requires implementable principles for privacy and trustworthiness.

Objective: This research has two interconnected objectives. The first is to define pervasive health as a system and to understand its trust and privacy challenges. The second goal is to build a conceptual model for pervasive health and use it to develop principles and polices which can make pervasive health trustworthy.

Methods: In this study, a five-step system analysis method is used. Pervasive health is defined using a metaphor of digital bubbles. A conceptual framework model focused on trustworthiness and privacy is then developed for pervasive health. On that model, principles and rules for trusted information management in pervasive health are defined.

Results: In the first phase of this study, a new definition of pervasive health was created. Using this model, differences between pervasive health and health care are stated. Reviewed publications demonstrate that the widely used principles of predefined and static trust cannot guarantee trustworthiness and privacy in pervasive health. Instead, such an environment requires personal dynamic and context-aware policies, awareness, and transparency. A conceptual framework model focused on information processing in pervasive health is developed. Using features of pervasive health and relations from the framework model, new principles for trusted pervasive health have been developed. The principles propose that personal health data should be under control of the data subject. The person shall have the right to verify the level of trust of any system which collects or processes his or her health information. Principles require that any stakeholder or system collecting or processing health data must support transparency and shall publish its trust and privacy attributes and even its domain specific policies.

Conclusions: The developed principles enable trustworthiness and guarantee privacy in pervasive health. The implementation of principles requires new infrastructural services such as trust verification and policy conflict resolution. After implementation, the accuracy and usability of principles should be analyzed.

(J Med Internet Res 2012;14(2):e52) doi:10.2196/jmir.1972

KEYWORDS

pervasive health; ubiquitous computing; privacy; trustworthiness; digital bubbles; conceptual modeling

Introduction

Health is a wider concept than absence of disease or poor functionality. Broadly, health covers a person's physical and mental, as well as economic and social, well-being. Therefore, health is not only a state determined by health care professionals and related authorities, but also an individually experienced state with many determinants, such as lifestyle, environment, social, and cultural aspects.

Traditionally, health care is an institutionalized and regulated system that occurs in controlled environments. The availability of information and communication technologies (ICT), ubiquitous computing, ambient intelligence, motes, sensors, and sensor networks is changing health care. New service models, such as personalized health care and personal health systems (PHS), are developing [1-2]. Ubiquitous health care is another new paradigm, which is closely related to biomedical engineering, health informatics, and ubiquitous computing [3]. It uses ubiquitous technology for continuously monitoring patients anywhere, for proactive prevention and early detection of diseases, and for ubiquitous access to medical data [4-6].

Ubiquitous computing technology, sensor networks, and ambient intelligence have initiated the birth of pervasive health. Pervasive health and health care are separate concepts with many overlapping goals (ie, making services available to everyone). They are not distinguished by the information technology or information used. Both can collect and deploy any kind of personal health data and environmental information (eg, genomic, phenomic, epigenetic, and geospatial information).

Trust and Information Privacy

Trust is a relativistic, complex, and dynamic concept. From the information-processing point of view, trust defines the individual's expectations in the context of collection, processing, communication, and use of personal information [7]. It allows acceptance of risk and balances privacy needs against benefits. Trust can be based on knowledge and experiences of an entity about actors and processes involved in personal data, on regulations established for ruling actors' behavior and processes, and on legislation binding actors and enforcing processes (law enforcement).

In the case of health information, trust defines the data subject's (DS) confidence that his or her personal health information is processed and communicated in such a way that privacy and security are guaranteed and the data processing follows regulations, ethical rules, fair information practices, and the DS's personal preferences.

Privacy is a multifaceted, relativistic, and context-dependent concept [8]. It has been defined by Westlin as the "claim of individuals, groups, and institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [9]. This paper focuses on the following privacy dimensions: right of informational self-determination and information privacy including privacy of personal behavior, freedom from surveillance, communication privacy, and data privacy [9-12]. Information privacy refers to a person's self-determination by respecting their wishes and demands regarding collection, processing, and communication of personal information, thereby preventing harm from disclosure.

Both information privacy and trust are related to the conditions demanded or expected in the collection, processing, communication, and use of personal information. Privacy policies, such as a patient's consent statement, explicitly express the DS's privacy requirements, while trust tackles them implicitly. Both privacy and trust relate to the information subject and include knowledge or assumptions about involved entities. Data disclosure means loss of privacy, but an increased level of trustworthiness reduces the need for privacy. The interest of the DS is to minimize loss of privacy at an acceptable level of trust.

Prior Work

In health care, internationally adopted principles and good practice rules—such as The United Nations (UN) Universal Declaration of Human Rights, the Organization for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems and Networks, the European Directive 95/46/EC known as the Data Protection Directive (DPD), and ethical guidelines and codes published by The World Medical Association and the International Medical Informatics Association (IMIA)—together approved the high-level frameworks for ethics and privacy protection [13-16]. International standardization organizations are also developing standards targeting secure processing of health information, such as the International Organization for Standardization's (ISO) Health informatics TC 215 standard [17,18]. Wassernaar reported that the following privacy principles are widely used: the principle of existence of privacy, the principle of withholdings, the principle of trusted usage, and the principle of controlled dissemination [12]. Langheinrich has proposed the following principles for privacy-aware ubiquitous systems: notice, choice and consent, proximity and locality, anonymity and pseudonymity, security access, and recourse [19]. His first principle, notice, is a subset of the awareness principle. Those documents and proposals stress that high-level policies such as withholding, trusted usage, controlled dissemination, legitimate grounds of processing, responsibilities of data processors, and purpose-based limitation are cornerstones in trusted information processing.

Researchers have recognized weaknesses and challenges in current privacy solutions. Coiera and Clark declared traditional access control systems inefficient because they are not content and context aware [20]. Anciaux et al identified that traditional electronic health records (EHR) have no security guarantee outside the health care service domain [21]. Ruotsalainen has pointed out that the patient has limited rights to control the use of EHRs [22]. Pallapa et al argued that systems using ubiquitous computing have no mechanism for people to reflect their intentions [23]. Mitseva et al noted that protection of privacy in sensor networks must support daily private life [24]. Hu and Weaver called current security and privacy solutions (based on a static role-based access control model) application dependent because they do not address new generations of eHealth requirements [25]. According to Joshi et al, security-based

authentication and role-based approaches are not sufficient in open systems [26]. Kim et al pointed out that informed consent is not possible in environments with a large amount of sensors [27].

New approaches have been proposed. Ball and Gold suggested that the individual should have control of their personal health record (PHR) and should be able to know who has entered which data into the record [28]. Kendall has proposed a patient-controlled EHR for the Information Age [29]. Kim et al recommended that data collection be under the sole control of the patient [27]. Haas et al proposed that the access and disclosure of EHRs be controlled by privacy policies [30]. They also stated that patients must be able to check how principles are implemented. Brown and Adams stated that the access to information should be under the control of the patient or the patient's guardian [31].

New principles and models have also been proposed. Solove pointed out that protection of privacy in the Information Age requires social design and an architectural solution [10]. Shankar et al stated that systems in a ubiquitous environment need dynamic- and context-based trust [32]. Kim et al recommended the use of a security policy that includes the following rules and principles: data collection must be under the sole control of the patient, a principle of disclosure, and principles of limitation and necessity [27]. Bhatti and Bhatti et al have pointed out that existing risks and the lack of common privacy and trust rules, regulations, and norms indicate that dynamic privacy rules are needed to make ubiquitous health care trusted [33,34]. Mandl et al and Huda et al have recommended personally controlled health records [35,36]. Shabo developed models for "patient-held records" with principles of personal control [37]. Coiera and Clarke developed models for e-Consent. One of those models is an active e-Consent system that can act as a gatekeeper [20]. Anonymization is proposed by Huda et al as a privacy tool [36]. Roger-France has developed a model of special gatekeepers that control the use of EHRs [38].

Not only researchers, but also international organizations and governments, have addressed the need for new rules. In a 2010 report to the president of the United States and to Congress, experts noted that current policies, such as the Health Insurance Portability and Accountability Act (HIPAA), leave many details vague. They also stated that tools and technologies are needed to empower individuals to manage their own health and that the definition for a formal privacy model is necessary [39]. The report also argued that current privacy policies and regulations are poorly specified and ineffective, and new mechanisms for trust management are needed. The American Medical Informatics Association (AMIA) has requested that every person have control over their own PHR (ie, all secondary uses of PHR data must be controlled by the person except as required by law) [40].

Although none of the proposal is targeted directly to pervasive health, they have addressed common aspects such as trustworthiness, awareness, and patient-/person-controlled use of the EHR/PHR.

Until now, pervasive health lacks a common definition, and principles—which can make it trusted—do not exist. In this paper, pervasive health is defined as a system. Principles, rules, and policies that guarantee the DS's privacy and information autonomy at the same time and make pervasive health trusted are proposed.

Methods

System analysis focuses on understanding a proposed system, identifying the problems, and recommending improvements. In this paper, "system" is understood as a group of independent elements that act together in a collective effort to achieve a goal. Pervasive health can be seen as a soft system because it involves social and cultural elements. In this study, a five-step system analysis method is used (similar steps can be found in the Soft Systems Methodology) to define pervasive health as a system and to develop privacy principles presented in this paper. The following steps were performed:

1. Defining the system in question (ie, pervasive health)

2. Identifying features and expressing problems of interest (eg, privacy and trustworthiness)

3. Discovering privacy risks and challenges in trustworthiness

4. Building a conceptual model for pervasive health

5. Developing improvements (ie, principles for trusted pervasive health)

Pervasive health is defined using the model (metaphor) of linked digital bubbles. The idea of digital bubbles was originally developed for pervasive environments and personal spaces [41]. A bubble is a digital territory and information walls between bubbles are virtual. A bubble includes one or more systems, their stakeholders, and the environment. Inside a bubble, systems have common privacy regulations and rules. The created high-level graphical model illustrates relations of bubbles in the information space. Features of pervasive health are derived from this model.

A conceptual model for pervasive health is developed using the recommended practice for architectural description of software-intensive systems created by the Institute of Electrical and Electronics Engineers (IEEE). The short name for this standard is IEEE 1471 [42]. Architecture in IEEE 1471 is the fundamental organization (eg, concepts and principles) of a system, its components, and their relationships. Using this method, a graphical framework model that describes trust- and privacy-related concepts and their relationships in pervasive health is developed.

In the final step of system analysis, principles for trusted pervasive health are developed by combining previously defined features of pervasive health, identified risks, selected high-level privacy principles, and their relationships described within the conceptual framework model.

Results

Definition of Pervasive Health

Figure 1 displays the developed graphical model for pervasive health. In this model, the information space is an open and

dynamic environment, which is characterized by the use of ubiquitous computing and by relations between bubbles. Its bubbles can be dynamically linked together, and information collecting and processing is poorly regulated (eg, privacy rules in bubbles are often unknown). In the case where a bubble includes many systems, they can have different business objectives, but they should have the same privacy regulations and rules.

Pervasive health is defined as a dynamic network of bubbles that offers health services to the person. In the information space, the person (DS) creates dynamically personal health networks and selects both systems that belong to the network and services used. The DS also defines what information is shared between bubbles and their systems. This means that pervasive health is a controlled (cybernetic) meta-system in the information space.

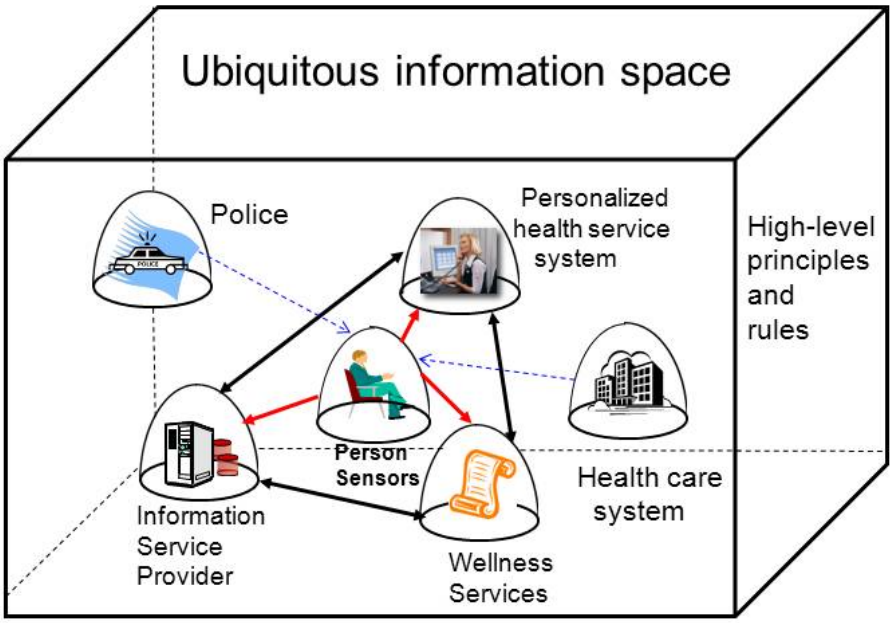
The current health care system can be understood as a bubble where public and private service providers offer health care services. In principle, those health care services which the DS uses outside the controlled health care environment can be part of the DS's pervasive health. Even so, the DS controls the use of those services and related data processing, except as required by law.

Despite the technology used and the available information, health care services are still defined, provided, and controlled by, health professionals targeting the patient [4]. Contrary to this, services of pervasive health and related data processing are controlled by the DS and the target is a person who can select, tailor, and combine autonomously their own health service portfolio with the help of intelligent services of the network.

In health care, security and privacy rules are regulated by domain-specific laws and norms, which is not the case in pervasive health. Furthermore, in pervasive health personal health data is not stored in institutionalized EHRs as we will discuss subsequently.

In the information space are also other systems which are not members of the DS's pervasive health network, but which are interested in using DS's health information (Figure 1). Those systems are called secondary users.

Figure 1. Pervasive health in the information space.



Information Processing and Storing in Pervasive Health

In the information space and in pervasive health, autonomous programs and computer systems can collect and process personal information invisible to the DS [19]. In pervasive health, both the information content and how it is collected, processed, and stored differ radically from current practice in health care. In the latter, patient data is recorded and used by health care professionals and typically managed by a service provider

organization in the form of the EHR [43]. In health care, the EHR can be used by professionals participating in the care of an individual, or by entities for purposes defined in legislation [22].

In pervasive health, those rules do not apply and health care-specific legislation will not regulate how health data is processed. In pervasive health, any kind of personal information (including behaviors and social activities) covering the person's entire life is collected and processed. The use of health data is not limited to patient care, treatments, public health, or clinical research. Systems of pervasive health can process and exchange personal health information using their own rules. The data content coming from multiple sources exceeds what is used in current health care (and what EHRs contain). The authors use the term "lifelong personal wellness record" (LPWR) for this information. Personal health record (PHR) is an alternative term. Unfortunately, there is no consensus about the concept of a PHR, and some writers see it as an extension of the regulated EHR [44]. Another proposal is that the PHR and the EHR should be integrated [45]. In this paper, the LPWR is defined as an independent repository, and the authors claim that the legal EHR does not replace either the PHR or the LPWR [46].

Privacy Threats in Ubiquitous Computing and in Pervasive Health

The information space and ubiquitous computing generate many privacy threats. The following are typical as stated in the literature [10,35,47]:

• Multiple systems and authorities can collect, process, and share personal information. Their number is unknown in advance and it changes regularly [20].

• There is no predefined trust between systems.

• Information can be collected, processed, and shared in such a way that the DS cannot be aware of it.

• Rich contextual metadata is collected and used, both violating the DS's privacy interests.

• Privacy can be breached if authorization is made without contextual information.

• It is difficult (or even impossible) to destroy data stored in the information space.

Pervasive health creates additional trustworthiness and privacy challenges:

• The business objectives, trust features, and regulations systems applied can be unknown.

• It is not possible to know in advance the characteristics, rules, and regulations of secondary users.

• Processing of the LPWR takes place in various contexts (situations).

• Objects of the LPWR can have different, situation-dependent sensitivity.

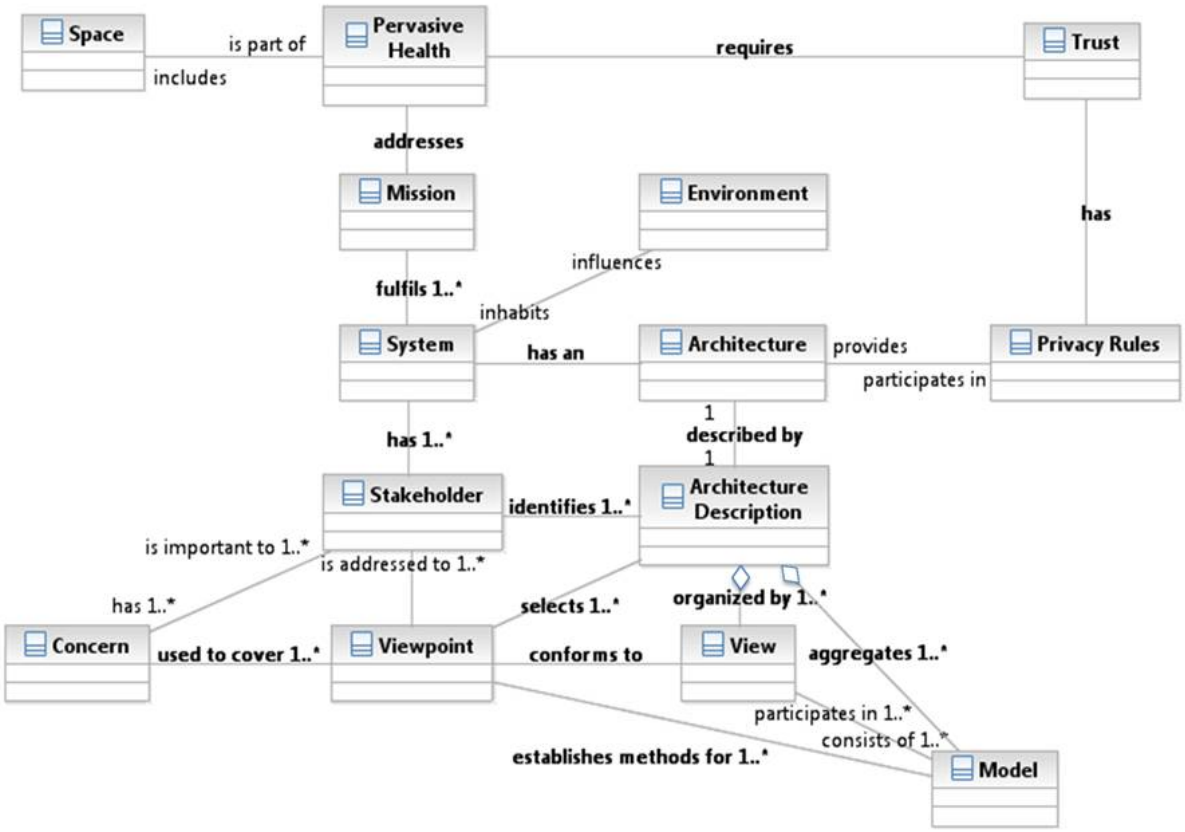
It is evident that, in pervasive health, the DS should be protected against the previously discussed risks and threats.

A Conceptual Model for Pervasive Health

The conceptual framework model developed is shown in Figure 2. The model links the key concepts of the authors' approach to pervasive health in the context of the research questions of data processing trustworthiness and information privacy.

Key concepts in the model are information space, pervasive health, trust, systems, stakeholders' interest/concerns, environment, and privacy. Environmental features in the model include regulatory issues. Features of the information space and its systems impact the existing level of trust. To be acceptable and effective, the pervasive health network requires that the level of trust that the DS needs, and what systems and stakeholders offer, be balanced.

Figure 2. Conceptual framework for pervasive health.



Stakeholders and Interests

Typical stakeholders (or actors) in pervasive health are the DS, wellness service providers, and data processing organizations. Stakeholders have different concerns or interests and viewpoints (eg, looking to meeting their business objectives, information availability, and usability). The DS's main interests are benefits of services, trustworthiness, and privacy and information autonomy. Also, conflicting interests can occur. For example, other systems in the information space, which are not members of the pervasive health array, might have interest in the DS's health information [48]. They collect and deploy health information for different kinds of secondary use, as demonstrated in Table 1.

Table 1. Typical primary and secondary uses of health data.

Primary u se	Secondary use
Direct care and treatment	Surveillance and continuous monitoring
Disease management	Research and statistics
Medication management	Drug development
Management of physical and social functionality for delaying of their weakening	Public health management
Proactive prediction of patient's health problems and prevention of diseases	Business application development
Management of patient's health status	Hindering behaviors not accepted by controllers (or authorities) or by society in general

Those secondary users are third parties such as public authorities, private organizations, community care providers, public health planners, communication vendors, employers, insurance institutes, researchers, and even homeland security organizations.

Principles for Trusted Pervasive Health

Trustworthiness in pervasive health means that the whole network of systems is trusted; the DS's privacy has been protected; and data is processed ethically, legally, and in line with the rules set by the DS. The resulting principles must offer

protection against risks of ubiquitous technologies, facilitate trustworthiness, and support the DS's information autonomy. As previously mentioned, the fact that there are no predefined common rules for privacy and trustworthiness in pervasive health should be also considered. Becker stated that specification documents, in real life, are unclear, ambiguous, and incomplete [49]. Therefore, principles should be more detailed and implementable than the previously discussed high-level principles.

From those privacy principles, the authors have selected trusted use and controlled dissemination, withholding, transparency, awareness, and the data processor's responsibility together with the principle of context-aware personal privacy as the basis for new principles and rules. This implies that the DS acts as a data controller and determines where, by whom, why, how, in which context, and to what extent, his or her personal health information is used and communicated (ie, the DS can define personal preferences and policies).

The following requirements have been derived from relationships in the framework model (Figure 2):

• All systems should fulfill the mission (ie, trustworthiness and privacy) and, therefore, they should accept common rules.

• Pervasive health requires trust. This implies the need for trust verification.

• Trust needs privacy rules.

The conceptual model also implies that the environment impacts the rules, and systems can use different rules. From the dynamic nature of the information space follows that the DS cannot be informed in advance which secondary users are using the LPWR.

The principles developed (named in this paper as THEWS principles for Trusted eHealth and eWelfare Space principles) are derived by combining selected principles and identified requirements. The THEWS principles state that the DS shall have the right to [50]:

• Dynamically verify the trustworthiness of the pervasive health network she has created.

• Verify the trustworthiness of any system in the information space that requires or uses the DS's personal health data for secondary purposes.

• Control the processing of personal health information, both inside systems and between them.

• Be aware of all events, situations, and contexts where the DS's health data is collected, processed, stored, and disclosed.

• Define situation-specific, context-aware, and granular personal privacy and trust policies, which regulate how his or her health data is collected, processed, disclosed, shared, stored, or destroyed.

Systems and stakeholders have the responsibility to ensure:

• Trust verification by publishing their privacy policies, environmental, and contextual features.

• Openness of their interest, business needs, and policies as well as their relationships with other systems in the information space.

• Transparency of data processing.

The THEWS principles imply that, in pervasive health, the entity DS is a person without an a priori assigned role as a patient or object of care. The DS should not only be aware of the use of his or her personal health data, but the DS also has to be able to verify trust and to control how data is collected, used, processed, and shared. Tables 2-4 demonstrate how the THEWS principles are related to high-level principles, and against which risks they offer protection.

Advance verification of trust is a prerequisite and it should be seen as a mandatory requirement, as shown in Table 2. For this purpose, all systems in the information space must publish their trust and privacy attributes or, even better, their policies.

Table 2. Principles of trust verification.

Privacy and trust risks [a]		THEWS principle	High-level privacy principle
	Unknown stakeholders' business needs, interest, purposes, and policies	Right to use trust verification	
	No predefined trust to any system	Mandatory to publish systems' trust parameters and policies	Trusted use of data
	Unknown secondary users	Trust level calculation	
	Invisible ubiquitous infrastructure	Untrusted systems and users cannot participate in the DS's health network	

[a] in the information space and in pervasive health

More closely, any system that collects health data or processes it shall publish the following information:

• Relevant regulations and ethical rules;

• Identification of all stakeholders who are participating to the data processing;

• Security and privacy features of computer systems and applications that can process the LPWR; and

• Agreements made between the system's stakeholders and other systems.

The principle of context-aware personal policy implies that the DS has the right to define dynamic personal privacy and security policies (thereby setting own privileges and obligations) for all systems and stakeholders regarding the collection, processing, and disclosure of its health data, as shown in Table 3. The DS can also define to what extent the content of the LPWR can be accessed by third parties and deployed for secondary uses. This principle is close to the theory of individual preference [49]. The principle of withholding is one dimension of the personal policy. Withholding means that the DS can modify, update, and delete any object in his or her LPWR at any time and from any place. Also, the "principle of acceptable reason" used in health care is part of the personal policy.

In pervasive health, the DS defines which reasons are acceptable for a situation in question. Therefore, reasons are a part of the policy. The DS's policy defines contexts and situations where the data can be processed; there is no necessity to use a separate concept of relationship (ie, the patient–doctor relationship). Furthermore, the "need to know" principle used in health care is not needed because permissions to use data are defined in the personal policy. The proposed model of personal policy also supports the following widely accepted privacy features: limitations of access, secrecy, control over personal information, personhood, and intimacy. Policies can be used to trigger situation-dependent acts such as anonymization of data and federation of access control. The principle of controlled data creation, processing, and disclosure is old. The new feature is that the DS's control is dynamic, context-aware, and linked to awareness and verification services.

Table 3. Principles of personal policies.

P rivacy and trust risks [a]		THEWS principle	High-level privacy principle
	The DS cannot control what health data is collected and by whom	Personal dynamic context-aware policies rule the collection, processing, storing, sharing, and destroying of data	Right to control the use of data
	The DS cannot control the use of the LPWR and its metadata	Possibility to control any secondary use of the LPWR and its metadata	
	No control over data linking	Policy defines rules for data linking and destroying as well as situations where the LPWR can be processed	Withholding
	Unknown secondary use of data		
	The information space has unlimited memory		

[a] in the information space and in pervasive health

In pervasive health, need for transparency is not limited to the processing of the LPWR, as shown in Table 4. It covers situations where data is collected or used as well as all contextual metadata. Furthermore, transparency means that a person should be aware of regulations, security features, and policies of systems and the organizations and computer applications that process, request, disclose, store, or destroy the DS's health data.

Table 4. Principles of awareness.

Privacy and trust risks [a]		THEWS principle	High-level privacy principle
	Invisible data collection, processing, preservation, and sharing	Awareness and transparency is defined by the DS's policy	
	No need to inform the DS the level of trust and of relations between systems	Stakeholders and systems shall publish their trust parameters and relations to other systems	Transparency
	No need to notify the DS of policy conflicts	Notification of conflicting interest and policies	

[a] in the information space and in pervasive health

Awareness covers activities such as browsing, mining and drilling, linking, and merging data at the granular level. Finally, the DS should be aware of all events where a conflict between his or her personal policy and the stakeholders' policy exists.

The THEWS principles are a paradigm shift from traditional static protection and risk-based thinking to dynamic management of trust and privacy. The principles offer new rights and power to the DS and, therefore, empower the DS's information autonomy. The principles also set new responsibilities to systems in the information space.

Discussion

In this paper, pervasive health is defined as a system that takes part in the information space. The trustworthiness and privacy challenges of pervasive health are analyzed. A conceptual model is built, and principles and rules, which can make pervasive

health trustworthy, are proposed. Principles give the DS the right to use personal polices and the right to verify trust. Full transparency and awareness give the DS power that currently does not exist. The THEWS principles protect the DS's health information against new, fast-developing technologies such as data mining, drilling, and browsing as well as against multidimensional profiling and re-identification. The use of dynamic policies makes it possible to balance on-the-fly access requester's purposes and the DS's personal preferences and policies. The authors' solution falls in line with modern policy and context-enabled security and privacy protection models developed for ubiquitous data processing [51].

The model of personal polices means that every person can have their own dynamic and context-dependent policies. This makes it difficult to manage policies and to automatically resolve their conflicts. A solution to this problem is the use of common privacy ontology and terminology. On that basis, it is possible to develop a set of policy profiles from where the DS can select the most suitable. It is also possible to allow the DS to simulate different policies and their impacts in advance. Policy conflicts between personal and local policies can be solved with the help of negotiation and conflict resolution services. A challenge is how the DS can make informed decisions to balance personal benefits with privacy and trust needs. One solution to this problem is the use of a software mediator between the DS and the access requestor or the health service provider [27].

A political challenge is getting the THEWS principles accepted by companies, governments, and health care organizations. The idea that the whole LPWR is under personal control of the DS in all situations may not be accepted by all stakeholders and systems automatically. Reasons for this include that it will make ICT systems expensive, complicated, and difficult to develop; it can cause problems for proactive prevention and make public health monitoring difficult; and it restricts governments' and bureaucrats' ability to monitor and control peoples' lifestyle and unwanted behaviors [19]. The THEWS principles also strengthen the person's autonomy and weaken common paternalism of current health care. Therefore, some health professionals will be resistant to these principles.

It is unclear whether all data subjects have reasonable interest or capacity to manage their personal security and privacy policies actively, or if some people will need a personal trust assistant to work on their behalf. From the regulatory viewpoint, there is a need to balance personal privacy and information autonomy against other interests and values, such as public and business benefits and secondary use of health data. New privacy regulations are also essential to trusted information space [52,53].

Implementing the THEWS principles requires services that do not exist currently. Both new infrastructural privacy services and a new data model for the LPWR are needed. The developed principles should be validated after implementation and their accuracy and usability should be analyzed.

Acknowledgments

Results presented in this paper are based on findings of the THEWS project (Trusted eHealth and eWelfare Space). The project is supported by the Finnish Academy during 2009-2012 via the MOTIVE research program.

Conflicts of Interest

None declared

References

1. Vogenberg FR, Barash CI, Pursel M. Personalized Medicine: Part 1: Evolution and Development into Theranostics. P&T 35 2010 Oct;35(10):560-576. [Medline: 21037908]
2. Kiefer S. European Commission Information Society. 2007. Personal Health Systems (PHS): Overview and research trends URL: http://ec.europa.eu/information_society/events/phs_2007/docs/slides/phs2007-kiefer-s1a.pdf [accessed 2012-03-19] [WebCite Cache ID 66HaxmDUN]
3. Bardram JE. Pervasive healthcare as a scientific discipline. Methods Inf Med 2008;47(3):178-185. [doi: 10.3423/ME9197] [Medline: 18473081]
4. Arnrich B, Mayora O, Bardram J, Tröster G. Pervasive healthcare: Paving the way for a pervasive, user-centered and preventive healthcare model. Methods Inf Med 2010;49(1):67-73. [doi: 10.3414/ME09-02-0044] [Medline: 20011810]
5. Varchney U. Pervasive healthcare. Computer 2003;36(12):138-140. [doi: 10.1109/MC.2003.1250897]
6. Codagnone C. European Commission Information Society. 2009 Aug. Reconstructing the whole: Present and future of personal health systems URL: http://ec.europa.eu/information_society/activities/health/docs/projects/phs2020/phs2020-book-rev16082009.pdf [accessed 2012-03-19] [WebCite Cache ID 66HaL4Eds]
7. Wanigasekera C, Feigenbaum J. Sensitive information in a wired world course (CS457). Newhaven, CT: Yale University; 2003 Dec 12. Trusted systems: Protecting sensitive information through technological solutions URL: http://zoo.cs.yale.edu/classes/cs457/backup/ [accessed 2012-01-27] [WebCite Cache ID 650H14LTe]
8. Lederer S, Deay AK, Mankoff J. UC Berkeley College of Engineering Technical Reports. Berkeley, CA: Computer Science Division, University of California; 2002 Jun. A conceptual model and metaphor of everyday privacy in ubiquitous computing environments URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2002/CSD-02-1188.pdf [accessed 2012-03-19] [WebCite Cache ID 66HZyp9vK]

9. Westin AF. Social and political dimensions of privacy. Journal of Social Issues 2003 Jul;59(2):431-453.
10. Solove D. The Digital Person: Technology and Privacy in the Information Age. New York, NY: New York University Press; 2004.
11. Wohlgemuth S, Muller G. Privacy with delegation of rights by identity management. In: Emerging Trends in Information and Communication Security Lecture Notes in Computer Science, 2006. Germany: Springler Verlang; 2006:175-190.
12. Wassernaar J. www.w3.org. 2006. Privacy rules, a steeple chase for systems architects URL: http://www.w3.org/2006/07/privacy-ws/papers/04-borking-rules/ [accessed 2012-01-27] [WebCite Cache ID 650I5cGMn]
13. European Commission. European Commission Justice Data Protection Policies. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [accessed 2012-01-27] [WebCite Cache ID 650KVEhUK]
14. United Nations. Geneva, Switzerland: United Nations; 2007. Universal Declaration of Human Rights URL: http://www.un.org/events/humanrights/2007/hrphotos/declaration%20_eng.pdf [accessed 2012-03-19] [WebCite Cache ID 66HYMvMaH]
15. Organisation for Economic Co-operation and Development (OECD). 2002. OECD guidelines for the security of information systems and networks: Towards a culture of security URL: http://www.oecd.org/dataoecd/16/22/15582260.pdf [accessed 2012-01-27] [WebCite Cache ID 650MSPyWi]
16. International Medical Informatics Association (IMIA). International Medical Informatics Association.: IMIA The IMIA Code of Ethics for Health Information Professionals URL: http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf [accessed 2012-01-27] [WebCite Cache ID 650N2Zm60]
17. International Organization for Standardization (ISO). ISO/IEC 27799 Health Informatics-Information Security Management in Health Using ISO/IEC 27002. Geneva, Switzerland: ISO; 2008.
18. International Organization for Standardization (ISO). ISO TS 22600 Health Informatics-Privilege Management and Access Control. Geneva, Switzerland: ISO; 2009.
19. Langheimreich M. Swiss Federal Institute of Technology Zurich. Zurich, Switzerland: Swiss Federal Institute of Technology (ETH) Privacy by design: Principles of privacy-aware ubiquitous systems URL: http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf [accessed 2012-03-27] [WebCite Cache ID 66U0efwZR]
20. Coiera E, Clarke R. e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment. J Am Med Inform Assoc 2004 Apr;11(2):129-140 [FREE Full text] [doi: 10.1197/jamia.M1480] [Medline: 14662803]
21. Anciaux N, Benzine M, Bouganim L, Jacquemin L, Pucheral P, Yin S. Restoring the patient control over her medical history. In: 21st IEEE Symposium on Computer-based Medical Systems. Los Alamitos, CA: IEEE Computer Society Press; 2008:132-137.
22. Ruotsalainen P. Security infrastructure services for patient managed lifelong health record. In: Travel Health Informatics and Telehealth: EFMI Special Topic Conference, Antalya, Turkey, 2009. Istanbul, Turkey: Victor Babes University Publishing House; 2009:51-29.
23. Pallapa G, Kumar M, Das K. Privacy infusion in ubiquitous computing, networking and services. In: Proceedings of MobiQuitous 2007. 2007 Presented at: MobiQuitous 2007; August 6-10, 2007; Philadelphia, PA. [doi: 10.1109/MoBIQ.2007.4451030]
24. Mitseva A, Wardana SA, Pradad NR. Context-aware privacy protection for wireless sensor networks in hybrid hierarchical architecture. In: Proceedings of International Wireless Communications and Mobile Computing 2008 Conference.: IEEE; 2008 Presented at: 2008 International Wireless Communications and Mobile Computing Conference; August 6-8, 2008; Crete Island, Greece. [doi: 10.1109/IWCMC.2008.134]
25. Hu J, Weaver AC. Pervasive Security, Privacy and Trust (PSPT4), August 2005. 2005. Dynamic, context-aware access control for distributed healthcare applications URL: http://www.cs.virginia.edu/~acw/security/doc/Publications/A%20Dynamic,%20Context-Aware%20Security%20Infrastructure% 20for%20Distri~1.pdf [accessed 2012-03-19] [WebCite Cache ID 66HVhI3rd]
26. Joshi A, Finin T, Kagal L, Parker J, Patwardhan A. Security policies and trust in ubiquitous computing. Philos Transact A Math Phys Eng Sci 2008 Oct 28;366(1881):3769-3780 [FREE Full text] [doi: 10.1098/rsta.2008.0142] [Medline: 18672450]
27. Stajano F, Kim HJ, Chae J, Kim S. Towards a security policy for ubiquitous healthcare systems (Position paper). In: Ubiquitous Convergence Technology First International Conference, ICUCT 2006, Jeju Island, Korea, December 5-6, 2006: revised selected papers. Berlin, Germany: Springer; 2007.
28. Ball MJ, Gold J. Banking on health: Personal records and information exchange. J Healthcare Inf Management 2006;20(2):71-83. [Medline: 16669591]
29. Kendall DB. Harvard Law and Policy Review. Protecting patient privacy in the information age URL: http://www.hlpronline.com/kendall.pdf [accessed 2012-03-19] [WebCite Cache ID 66HVTSzjj]
30. Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller G. Aspects of privacy for electronic health records. Int J Med Inform 2011 Feb;80(2):e26-e31. [doi: 10.1016/j.ijmedinf.2010.10.001] [Medline: 21041113]
31. Brown I, Adams AA. The ethical challenges of ubiquitous healthcare. International Review of Information Ethics 2007;8:53-60 [FREE Full text] [WebCite Cache]

32. Shankar N, Balfanz D. Enabling secure ad-hoc communication using context-aware security services. In: Proceedings of UBICOMP 2002-Workshop on Security in Ubiquitous Computing. 2002 Presented at: UBICOMP 2002; 2002; Gothenburg, Sweden URL: http://www.teco.edu/~philip/ubicomp2002ws/organize [WebCite Cache]
33. Bhatti R. X-GTRBAC: An XML-based policy specification framework and architecture for enterprise-wide access control. ACM Transactions on Information and System Security 2005;8(2):187-227. [doi: 10.1145/1065545.1065547]
34. Bhatti R, Moidu K, Ghafoor A. Policy-based security management for federated healthcare databases (or RHIOs). In: HIKM '06 Proceedings of the International Workshop on Healthcare Information and Knowledge Management. New York, NY: ACM; 2006.
35. Mandl KD, Simons WW, Crawford WC, Abbett JM. Indivo: a personally controlled health record for health information exchange and communication. BMC Med Inform Decision Making 2007;7(25) [FREE Full text] [doi: 10.1186/1472-6947-7-25] [Medline: 17850667]
36. Huda MN, Sonehara N, Yamada S. Journal of Engineering Science and Technology (JESTEC). 2009. A privacy management architecture for patient-controlled personal health record systems URL: http://jestec.taylors.edu.my/Vol%25204%2520Issue%25202%2520June%252009/Vol_4_2_154-170_MD_NURUL_HUDA.pdf [accessed 2012-03-19] [WebCite Cache ID 66HUH8rwr]
37. Shabo A. A global socio-economic-medico-legal model for the sustainability of longitudinal electronic health records. Part 1. Methods Inf Med 2006;45(3):240-245. [Medline: 16685331]
38. France F. eHealth in Belgium, a new "secure" federal network: role of patients, health professions and social security services. Int J Med Inform 2011 Feb;80(2):e12-e16. [doi: 10.1016/j.ijmedinf.2010.10.005] [Medline: 21035383]
39. President's Council of Advisors on Science and Technology (PCAST). The White House. Washington, DC; 2010 Dec. Report to the President and Congress: Designing a digital future: Federally funded research and development in networking and information technology URL: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf [accessed 2012-03-19] [WebCite Cache ID 66HipPled]
40. American Health Information Management Association and American Medical Informatics Association. The value of personal health records: A joint position statement for consumers of health care. In: Bos L, Blobel B, Marsh A, Carroll D, editors. Medical and Care Compunetics 5 (Technology and Informatics). Amsterdam, Netherlands: IOS Press; 2008.
41. Kapadia A, Henderson T, Fielding JJ, Kotz D. Virtual walls: Protecting privacy in pervasive environments. In: Proceedings Pervasive Computing, 5th International Conference, PERVASIVE 2007. Berlin: Springler Verlag; 2007 Presented at: The 5th International Conference on Pervasive Computing; May 13-16, 2007; Toronto, Ontario. [doi: 10.1007/978-3-540-72037-9_10]
42. Institute of Electrical and Electronics Engineers (IEEE) Computer Society. IEEE Standard 1471-2000: Recommended Practice for Architectural Description of Software-Intensive Systems. Piscataway, NJ: IEEE; 2000.
43. National Electronic Health Records Taskforce, Commonwealth of Australia. A health information network for Australia. In: Report to Health Ministers by the National Electronic Health Records Taskforce. Australia: Minister of Health; 2000.
44. US Department of Health and Human Services. National Committee on Vital and Health Statistics. 2006. Personal health records and personal health record systems: A report and recommendations from the National Committee on Vital and Health Statistics URL: http://ncvhs.hhs.gov/0602nhiirpt.pdf [accessed 2012-03-19] [WebCite Cache ID 66HRqyKAr]
45. Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc 2006;13(2):121-126 [FREE Full text] [doi: 10.1197/jamia.M2025] [Medline: 16357345]
46. Detmer D, Bloomrosen M, Raymond B, Tang P. Integrated personal health records: transformative tools for consumer-centric care. BMC Med Inform Decis Mak 2008;8:45 [FREE Full text] [doi: 10.1186/1472-6947-8-45] [Medline: 18837999]
47. Samarati P, Bertino E, Jajodia S. An authorisation model for distributed hypertext system. IEEE Transactions on Knowledge and Data Engineering 1996;8(4):555-562. [doi: 10.1109/69.536249]
48. Safran C, Bloomrosen M, Hammond WE, Labkoff S, Markel-Fox S, Tang PC, Expert Panel. Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. J Am Med Inform Assoc 2007;14(1):1-9 [FREE Full text] [doi: 10.1197/jamia.M2273] [Medline: 17077452]
49. Becker MY. A formal security policy for an NHS electronic health record service. In: University of Cambridge, Technical Report number 628, March 2005. London, UK: University of Cambridge; Mar 01, 2005.
50. Ruotsalainen P, Blobel B, Nykänen P, Seppälä A, Sorvari H. Framework model and principles for trusted information sharing in pervasive health. Stud Health Technol Inform 2011;169:497-501. [Medline: 21893799]
51. Blobel B, Nordberg R, Davis JM, Pharow P. Modelling privilege management and access control. Int J Med Inform 2006 Aug;75(8):597-623. [doi: 10.1016/j.ijmedinf.2005.08.010] [Medline: 16199198]
52. European Commission. Brussels, Belgium: European Commission; 2010 Apr 11. Communication from the Commission to the European parliament, the council, the economic and social committee and the committee of the regions: A comprehensive approach on personal data protection in the European Union URL: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf [accessed 2012-03-27] [WebCite Cache ID 66U8qB7LI]
53. Hussain S, Yang LT, Laforest F, Verdier C. Pervasive health care services and technologies. Int J Telemed Appl 2008;946082 [FREE Full text] [doi: 10.1155/2008/946082] [Medline: 18825271]

Abbreviations

AMIA: American Medical Informatics Association
DPD: Data Protection Directive
DS: data subject
EHR: electronic health records
HIPAA: the Health Insurance Portability and Accountability Act
ICT: information and communication technologies
LPWR: lifelong personal wellness record
OECD: Organization for Economic Co-operation and Development
PHR: personal health record
PHS: personal health systems
THEWS: Trusted eHealth and eWelfare Space
UN: United Nations
WHO: World Health Organization

Edited by G Eysenbach; submitted 25.10.11; peer-reviewed by S Koch, P Chhanabhai; comments to author 16.11.11; revised version received 02.02.12; accepted 09.03.12; published 30.03.12

Please cite as:
Ruotsalainen P, Blobel B, Seppälä A, Sorvari H, Nykänen P
A Conceptual Framework and Principles for Trusted Pervasive Health
J Med Internet Res 2012;14(2):e52
URL: http://www.jmir.org/2012/2/e52/
doi:10.2196/jmir.1972
PMID:

MEDINFO 2013
C.U. Lehmann et al. (Eds.)

doi:10.3233/978-1-61499-289-9-219

Feasibility Analysis of the Privacy Attributes of the Personal Wellness Information Model

Pirkko Nykänen[a], Antto Seppälä[a], Pekka Ruotsalainen[a] , Bernd Blobel[b]

[a] *School of Information Sciences, Center for Information and Systems, University of Tampere, Finland*
[b] *eHealth Competence Center, University Hospital Regensburg, Germany*

Abstract

A feasibility analysis has been performed to study the applicability of privacy attributes with a developed wellness information model. Information privacy concerns specifically access to individually identifiable personal information and one's ability to control information about oneself. We carried out a user scenario walk-through of the privacy attributes related to the wellness components. The walk-through showed a need to relate self-regulating privacy policies to the pervasive context so that during various trust-building processes, a person is aware and can control the use, disclosure and even secondary use of his personal, private wellness information.

Keywords:

Feasibility, privacy, personal wellness, information model.

Introduction

A feasibility study is an important phase in the development of models and services. The ultimate goal of a feasibility study is to outline and clarify the things and factors connected to developed models and solutions [1]. This kind of study collects information and evidence on the feasibility of research results before the results are actually implemented in practice. Thus, the feasibility study provides the proof-of-the concept, information for further planning and refinement and it forms the framework for further system development project and for further studies.

The phases in our preliminary feasibility study were planned following the GEP-HI evaluation guideline [2]: preliminary study planning with the purpose to outline and analyze the attributes and factors of interest of the wellness information model with related privacy concepts; study implementation planning to select the analysis criteria and methods; execution of the study, and reporting of the complete study following the STARE-HI guideline [3]. This paper presents a short summary of the proof-of-concept phase of our feasibility study.

Materials and Methods

The model and privacy attributes

The wellness information model aims at covering the essential aspects of personal wellness information. Major components of the model are: Emotional and mental wellness, occupational wellness, environmental factors, social networks, lifestyle aspects, physiological information, and health care service (Figure 1). The components are further divided into concept classes and sub concepts.

The wellness information model has been developed in a 4-year research project[1] with literature analyses and empirical research [4-6]. The interesting components of our feasibility study are: Health care services provision, lifestyle, social networks, and emotional and mental wellness. These were selected to be objects in our analysis because they summarize well the aspects of the holistic health and wellness. Many wellness models in the literature remain at very high-level and traditional health care related models or ontologies focus on specific diseases or medical conditions and do not consider the holistic view of wellness and health [7-11]. Today issues of lifestyle and social networks are more and more important for persons in their wellness management and control [12-13]. Also in our empirical focus groups, the social networks and lifestyle aspects were emphasized by the participating persons [4-5].

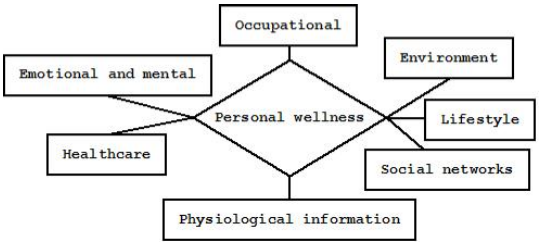


Figure 1- Major components of the personal wellness model

Information privacy has become a very important issue with the growth of ubiquitous computing which allows many options for collecting and using personal information. Also, the global and open nature of the Internet enables easy collection, storage and utilization of personal information [14]. In health care environment, information privacy is especially important as personal health information is confidential and should be protected from un-authorized use, access, and disclosure. Privacy concerns rise from the growing interest for reuse and for secondary use of personal information for other purposes; it was originally collected in modern dynamic environments [14-17].

Privacy refers to person's ability to control the collection, use and dissemination of one's personal information [15]. Westin [17] sees the communication aspect important in privacy by emphasizing privacy as the claim of individuals, groups, and institutions to determine for themselves when, how, and to

[1] Trusted eHealth and eWelfare Information Space (THEWS)

what extent information about them is communicated to others. Personal information is always related to the social context where the privacy issues are raised and challenged [18-19]. The socio-technical aspect of privacy means that the users should be aware of the type of information collected, exchanged and processed in order to be able to make choices regarding who, why, and where his/her personal information can be used.

Privacy is a personal and situation depending concept. Therefore, "good/bad privacy" seems to be just a qualitative opinion. A better approach is to measure the privacy level or attributes. Privacy metrics can be used to assess the degree to which a particular ubiquitous application complies with privacy requirements. Metrics suggested in [20] provide options: no control (0), control over disclosure of one kind of information (1), control over two kinds of information (2), and control over all three kinds of information (3). The types of information covered by this metrics are contents, location, and identity.

Trust is an interrelated variable to information privacy; trust is mediating between information privacy and willingness to disclose private information [14]. In a contextual situation, trust and needed level of privacy are interrelated and increased level of trustworthiness reduces the need for privacy [21-22].

In relation to the wellness concepts, we defined the privacy attributes for each concept in Table 1. The attributes are based partly on our empirical research [4-6] and partly on the performed recent literature search which covered electronic literature databases with keywords: privacy, personal wellness, and pervasive health. We identified attributes which are further studied in this feasibility analysis with the specific focus on the personal wellness information [21-22]. The motivation was to have a deeper understanding on privacy. Earlier research has been much focused on types of privacy information, on privacy metrics, and policies; privacy attributes have so far been not much discussed [14-17].

Table 1 - Privacy attributes of the selected wellness components

Wellness model component	Privacy attributes
Health care	Context, capability, competence, reliability, benefit, benevolence, confidence
Lifestyle	Context, confidence, reliability, benefit, value
Social networks	Context, confidence, reliability, benefit, value
Emotional and mental wellness	Context, confidence, reliability, benefit, value

The meanings of the attributes come from IT literature. Context refers to type or domain of the research, to the phenomena that exist in the environment, time (when), location (where), occupation (who), culture (with whom), and rationale (why) [23]. Capability refers to the ability of the information entity to show the attribute values, competence presents the level of privacy demonstration, and reliability describes how reliable information or source is considered by a person. Benefit presents the privacy benefits and confidence describes how confident the user is with information. Benevolence is the extent to which an individual is perceived to have good intention toward others without profit motive [24]. Value presents how valuable privacy is considered by a person in action or activity.

The framework and analysis method

The theoretical framework for our study is the design science intent of IT with the focus on conceptualization and representation of real problems and on implementation and evaluation of solutions using appropriate criteria [25-26]. Design science attempts to create things that serve human purposes and its products are assessed against criteria of value or utility - does it work? Is it an improvement?

In our research, we have aimed to produce as outputs concepts and a model. The personal wellness model identifies relevant concepts and thus presents a vocabulary of personal wellness. Following from the framework, our analysis questions are: Are the created wellness concepts better than the old ones, i.e. those presented in previous research and literature? Does our wellness model give a feasible classification for concepts and does it relate the privacy attributes to the concepts? Do these attributes cover the required privacy needs? Does the wellness model contribute to having a better understanding of personal wellness, its contents and limits?

The first step in our feasibility analysis was to analyze the concepts. The method for concept development was an analysis of earlier published research. We searched for published articles with keywords personal health, pervasive health, wellness, welfare, and information model [4-6]. The second step was to analyze the developed conceptual model with related privacy attributes. The method applied in this analysis was an empirical user scenario walk-through to study the feasibility of the related privacy attributes.

Results

The conceptual analysis has been performed and reported in detail in [5]. The results show that the concepts in our wellness model describe the personal wellness domain in more detail than models presented in the literature do. We have presented more concepts, relationships and properties in the model than the earlier general models did. The focus in our model is broader as we address the wellness from the information systems science perspective with the purpose to present a model that enables implementation [5].

For the second step, we developed a user scenario to walk through the selected model components in order to analyze the privacy attributes related to these wellness components. The scenario with privacy attributes is presented in Table 2. The privacy attributes with the components originate both from non-regulated and regulated contexts and privacy and trust in the non-regulated context are not ensured. However, the personal value of the attributes is high and they are considered highly beneficial. This gives a mixed situation between regulated and non-regulated contexts for personal wellness information. The person involved in pervasive wellness environment wants to be aware and wants to control his/her personal information, its use, access and disclose, and he/she would need ensured means to achieve this.

In our analysis, we walked through all the four selected wellness information model components. As an example, a more detailed analysis of the privacy attributes of the lifestyle component scenario is presented in Table 3. As privacy specifically concerns one's ability to control information about oneself, we have studied the privacy attributes in the walk-through from this ability-to-control perspective.

Table 2 – User scenario with components and related privacy attributes – A person, 50-year old healthy, employed man, diagnosed as diabetes mellitus type 2 (DM T2)

Model component	**Activity / Action**	**Privacy attributes**	
		Attribute	**Contents**
Health care	Receives treatment, medication and guidance for home care of DM T2	**Context**	regulated
		Capability	capable to provide privacy and trust
		Competence	assumed to be high
		Reliability	organization-based trust
		Benefit	high personal benefit
		Benevolence	good intention
		Confidence	required procedures, standards and safeguards have been implemented
Lifestyle	Starts to improve his lifestyle, uses a personal wellness diary system in PC	**Context**	non-regulated
		Confidence	reputation-based
		Reliability	past history-based
		Benefit	high personal benefit
		Value	high personal value
Social networks	Searches for peer-support in the Internet, and for information on DM T2	**Context**	non-regulated
		Confidence	reputation-based
		Reliability	past history-based
		Benefit	personal benefit considered high
		Value	personal value considered high
Emotional and mental wellness	Searches for recovery from depressed moods and support for higher spirits	**Context**	non-regulated
		Confidence	reputation-based
		Reliability	past history-based
		Benefit	personal benefit considered high
		Value	personal value considered high

The walk-through clearly shows that in the pervasive context, it is difficult for a person to know what the actual privacy status of the service or the service provider is, especially when the provider is a non-regulated one such as lifestyle or social networks. The walk-through also shows that the person does not have trust on privacy of the non-regulated information and its reliability is not controlled by the person.

Table 3 –Details of the lifestyle component walk-through

User actions	**Privacy attribute – one's ability to control**
Person searches for information on DM T2, on medication and treatment, on healthy life style, on peer support in the Internet	Context – Internet, non-regulated – ability to control: only with certified sites which provide trust, other sites: no control
	Confidence – certificates provide some confidence, otherwise: confidence does not exist
	Reliability – certified sites are considered somewhat reliable, otherwise reliability does not exist
	Benefit – benefit is considered high, controlled by a person
	Value – Information value is high, very meaningful for the person, the value is determined and controlled by the person
Person starts a healthy diet and documents his eating and blood sugar levels in his own wellness diary in a PC	Context – non-regulated, control by the person (what to document, where to documen, when to document)
	Confidence – the person may /or may not be confident (depending on his abilities and on the security status of his/her PC)
	Reliability – PC reliability is controlled normally by PC security service provider, sometimes by a person, blood glucose meter reliability is not controlled by a person
	Benefit – benefit is considered high, controlled by a person
	Value – high value for the person's DM management and healthy lifestyle
Person stores the data he receives from a doctor into his notebook (diagnosis, medication, treatment guidelines) for his personal use	Context – data is coming from regulated context, stored in non-regulated context, person controls (what, where)
	Confidence – the person may /or may not be confident (depending on his abilities and on the security status of his/her notebook)
	Reliability – data is considered reliable, high trust by the person (data is transferred from an organizational trusted source)
	Benefit – benefit is considered high, controlled by a person
	Value – high value, important for home care, for DM management and healthy lifestyle

Our analysis shows that when information is transferred from regulated source to non-regulated source, the information is considered to be reliable when the person trusts that the required procedures, standards, and safeguards have been implemented for data security and privacy management. However, after the data is transferred, the original data security and privacy policies and values of privacy attributes are no longer valid. The same situation concerns certified Internet sites; when a person receives the third party certificate, he/she has

high trust and confidence on the reliability of the site. When a person is accessing lifestyle information from non-certified sites, there is no trust on the privacy and no reliability on the information source.

Discussion

To achieve good privacy status, the non-regulated and regulated domains need to be integrated in such way that the person having health and wellness services is always aware and can control the privacy status of the services he/she uses. The person wants to be confident, to have trust on the privacy of his/her wellness information in all situations. For this purpose, we need to develop special privacy services for non-regulated environment that can be integrated with the regulated service access and disclose [23-24].These special services enable users to monitor privacy attributes, to connect metrics to them, and to measure the degree to which the users have control over their private information.

This research suggests incorporating trust-building measures to the non-regulated context. Examples of trust-building measures are third party certificates, branding, owner disclosure which means explicitly presenting the ownership or the sponsorship of the context, self-regulating policies that explicate the rules and guiding principles of the context, and source disclosure that identifies the source of information presented [24]. With pervasive health, the self-regulating policies are the most essential, other measures are more applicable to health information websites. A self-regulating policy means that for each concept in the wellness information model, the privacy attributes are defined. In all cases, when the concept is accessed, stored, processed, or transferred, the privacy attribute values are activated and made known, controllable and measurable.

This is a process-driven approach for a dynamic, context-sensitive ubiquitous environment as the trust-building measure is always related to the trust-building processes [24] such as calculative, predictive, intentionality, capability, and transference processes. For personal wellness information, important and essential processes would be the predictive, intentionality, capability and transference processes. Predictive trust building in pervasive health means reputation-based trust-building; a person can build trust if he/she knows about the past behavior of the pervasive service. Intentionality, process would mean that trust can be developed if we have perceptions on the intensions of the service or service provider. Capability based trust building requires that a person is able to evaluate the ability of the service or service provider to deliver the service. Finally, the transference process refers to a situation when information is transferred from a regulated context to the non-regulated pervasive health context.

With all these processes, the self-regulating policies are needed to explicate the rules and guiding principles in the context. With our wellness information model, self-regulating policies mean that we define the privacy attributes for each concept of the components and connect privacy measure to the attribute.

Management of personal information privacy is important as many studies [11, 14-17] indicate that privacy is a top reason for citizens' reluctance to adopt personal health and wellness systems. Privacy is also the driver for non-regulated health service business model. Many of the existing personal health systems do not cover privacy and security regulations for health information or services. For citizens, this means low trustworthiness that their data and information are properly protected. A recent study [27] shows that personal dispositions should be taken into consideration when examining privacy concerns and behavioral intentions to disclose health information online or in pervasive environment. This opens new and interesting paths for the future research, e.g. study of personalized privacy measures and processes to support personally each individual in pervasive environment.

Conclusions

Our feasibility analysis questions were: Does our wellness model relate the privacy attributes to the concepts? Do these attributes cover the required privacy needs? This is an additional request to the previous models presented in the literature. Our developed wellness model represents essential concepts and gives a structure to the presentation. The model can be used to build instantiations. If the model helps both the user and the developer to better understand the problem at hand, or to develop better instantiations based on better understanding, the model gives more possibilities than the earlier ones. However, the problem in the model is the mix of regulated and non-regulated information access, use and disclose. The currently regulated privacy regulations do not support this kind of pervasive health and wellness information environment [21].

We have analyzed the status of the privacy attributes with a restricted scenario walk-through and have found that the attributes presented help a person to be aware of, to control and to measure the privacy of his/her personal wellness information. The attributes emphasize the dynamic characteristics of the wellness information model in the pervasive health environment. However, in the non-regulated environment, we need technical solutions on how these attributes are managed and made known, available, and controllable.

Our research has shown that trust-building processes are needed to ensure the trust development. Information privacy is not yet properly managed in non-regulated environments and many challenges are offered by the personal health systems which often integrate data from regulated and non-regulated sources. These systems may be very beneficial for citizens and therefore privacy and trust concerns are essential and require solutions. This research has presented an approach for definition and management of privacy attributes with personal information models. Though this is a restricted study, we have provided contribution to information privacy research in two important aspects: applying design science approach and approaching the privacy attributes from the users' perspective. These issues have not been included in most information privacy research as Belanger and Crossler [15] found in their extensive information privacy research review. These findings call for further research to study all potential approaches and to find innovative, feasible and implementable solutions for information privacy in pervasive health.

Acknowledgments

The authors acknowledge the funding of Trusted eHealth and eWelfare Information Space (THEWS) research by the Finnish Academy of Sciences in the MOTIVE Research Programme during 2009-2012.

References

[1] Bryce T, The elements of good feasibility study. http://www.projectsmart.co.uk/pdf/elements-of-a-good-feasibility-study.pdf (Accessed 1.12.2012).

[2] Nykänen P, Brender J, Talmon J, de Keizer N, Rigby M, Beuscart-Zephir MC, Ammenwerth E, Guideline for good evaluation practice in health informatics (GEP-HI). Int J Med Inform 2011: 80(12):815-27.

[3] Talmon J, Ammenwerth E, Brender J, de Keizer N, Nykänen P, Rigby M, STARE-HI – Statement on reporting of evaluation studies in health informatics. Int J Med Inform 2009:78:1-9.

[4] Seppälä A, Nykänen P, Contextual analysis and modeling of personal wellness. In: Filipe J and Dietz JLG (Eds.), KEOD 2011, Proceedings of the International Conference Knowledge Engineering and Ontology Development. Paris, France, 26-29 October 2011: SciTePress - Science and Technology Publications, 2011, 202-207.

[5] Seppälä A, Nykänen P, Ruotsalainen P, Development of personal wellness information model for pervasive healthcare. Journal of Computer Networks and Communications, 2012, Article ID 596749, 10 pages, doi:10.1155/2012/596749.

[6] Nykänen P and Seppälä A, Collaborative approach for sustainable citizen-centered health care. In: N Wickramasinghe, R K Bali, S Kirn and R Suomi (Eds.), Critical issues of sustainable E-health solutions. Health care delivery in the information age. Springer Verlag, 2012, 115-134.

[7] Myers JE and Sweeney TJ, The indivisible self: an evidence-based model of wellness. Journal of Individual Psychology, 2004: 60(3): 234–245.

[8] Soomlek C and Benedicenti L, Operational wellness model: a wellness model designed for an agent-based wellness visualization system. 2nd International Conference on eHealth,Telemedicine, and Social Medicine (ETELEMED '10), 2010, 45–50.

[9] Kirsten TGJC, van der Walt HJL and Viljoen CT, Health, well-being and wellness: an anthropological ecosystemic approach, Health SA Gesondheid, 2009: 14: 1–7.

[10]Schuster TL, Dobson M, Jauregui M and Blanks RHI, Wellness lifestyles: a theoretical framework linking wellness, health lifestyles, and complementary and alternative medicine. Journal of Alternative and Complementary Medicine, 2004: 10(2): 349–356.

[11]Codagnone C, Reconstructing the Whole: Present and Future of Personal Health Systems, PHS2020, European Commission, 2009,

http://ec.europa.eu/information_society/activities/health/docs/projects/phs2020/phs2020-book-rev16082009.pdf (Accessed 25.11.2012).

[12]Denecke, K and Nejdl, W, How valuable is medical social media data? Content analysis of the medical web. Information Sciences, 2009: 179: 1870-1880.

[13]Eysenbach, G, Medicine 2.0: Social Networking, collaboration, participation, apomediation, and openness. Journal of Medical Internet Research, 2008: 10: 3, e22.

[14] Pavlou PA, State of the information privacy literature: where are we now and where should we go? MIS Quarterly 2011: 35(4): 977–988.

[15]Belanger F, Crossler RE, Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly, 2011:35(4):1017–1041.

[16]Smith JH, Dinev T and Xu H, Information privacy research: an interdisciplinary review. MIS Quarterly, 2011, 35(4): 989-1015.

[17]Westin A, Social and political dimensions of privacy. J Social Issues, 2003: 59(2): 431–453.

[18]Rallapalli M, Trust factors in privacy framework enabled socio-technical systems. Int J of E-Business Development, 2012: 2(4): 165-169.

[19]Nissenbaum H, Privacy in context: Technology, policy and the integrity of social life. Stanford University Press, USA, 2010.

[20] Jafari S, Mtenzi F, O'Driscoll C, Fitzpatrick R and O'Shea B, Measuring privacy in ubiquitous computing applications. Int J of Digital Society, 2011: 2(3):547-550.

[21]Ruotsalainen P, Blobel B, Nykänen P, Seppälä A, Sorvari H, Framework model and principles for trusted information sharing in pervasive health. In: A Moen, SK Andersen, J Aarts and P Hurlen (eds.), User Centred Networked Health Care. Proceedings of the MIE2011, Oslo, IOS Press, Amsterdam, 2011, 497-501.

[22]Ruotsalainen P, Blobel B, Seppälä A, Sorvari H, Nykänen P, A Conceptual Framework and Principles for Trusted Pervasive Health. J Med Internet Res 2012: 14(2):e52

[23]Bansal G, Zadehi F and Gehen D, The moderating influence of privacy concerns on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. In: Proc. of the 29th Int Conference on Information Systems (ICIS2008), Paris, 2008.

[24]Luo W and Najdawi M, Trust-building Measures: A Review of Consumer health portals. Communications of the ACM, January 2004: 47(1):109-113.

[25]March ST and Smith GF, Design and natural science research on information technology. Decision Support Systems, 1995: 15(4): 251–266.

[26]Hevner AR, March ST, Park J and Ram S, Design science in information systems research. MIS Quarterly, 2004:28(1): 75-105.

[27]Bansai G, Zahedi FM, Gehen D, The impact of personal dispositions on information sensitivity, privacy concerns and trust in disclosing health information. Decision support systems, 2010: 49(2): 138-160.

Address for correspondence

Pirkko Nykänen, University of Tampere, School of Information Sciences, PO Box 607, FIN-33014 Email: Pirkko.Nykanen@uta.fi, GSM +358 40 1901 720.

Original Paper

Trust Information-Based Privacy Architecture for Ubiquitous Health

Pekka Sakari Ruotsalainen[1*], DSc (Tech); Bernd Blobel[2*], PhD; Antto Seppälä[1*], MSc; Pirkko Nykänen[1*], PhD

[1]School of Information Sciences, Center for Information and Systems, University of Tampere, Tampere, Finland

[2]eHealth Competence Center, University Hospital Regensburg, University of Regensburg, Regensburg, Germany

[*]all authors contributed equally

Corresponding Author:
Pekka Sakari Ruotsalainen, DSc (Tech)
School of Information Sciences
Center for Information and Systems
University of Tampere
Kanslerinrinne 1
Tampere, 33014
Finland
Phone: 358 505 004 046
Fax: 358 405261336
Email: pekka.ruotsalainen@uta.fi

Abstract

Background: Ubiquitous health is defined as a dynamic network of interconnected systems that offers health services independent of time and location to a data subject (DS). The network takes place in open and unsecure information space. It is created and managed by the DS who sets rules that regulate the way personal health information is collected and used. Compared to health care, it is impossible in ubiquitous health to assume the existence of a priori trust between the DS and service providers and to produce privacy using static security services. In ubiquitous health features, business goals and regulations systems followed often remain unknown. Furthermore, health care-specific regulations do not rule the ways health data is processed and shared. To be successful, ubiquitous health requires novel privacy architecture.

Objective: The goal of this study was to develop a privacy management architecture that helps the DS to create and dynamically manage the network and to maintain information privacy. The architecture should enable the DS to dynamically define service and system-specific rules that regulate the way subject data is processed. The architecture should provide to the DS reliable trust information about systems and assist in the formulation of privacy policies. Furthermore, the architecture should give feedback upon how systems follow the policies of DS and offer protection against privacy and trust threats existing in ubiquitous environments.

Methods: A sequential method that combines methodologies used in system theory, systems engineering, requirement analysis, and system design was used in the study. In the first phase, principles, trust and privacy models, and viewpoints were selected. Thereafter, functional requirements and services were developed on the basis of a careful analysis of existing research published in journals and conference proceedings. Based on principles, models, and requirements, architectural components and their interconnections were developed using system analysis.

Results: The architecture mimics the way humans use trust information in decision making, and enables the DS to design system-specific privacy policies using computational trust information that is based on systems' measured features. The trust attributes that were developed describe the level systems for support awareness and transparency, and how they follow general and domain-specific regulations and laws. The monitoring component of the architecture offers dynamic feedback concerning how the system enforces the polices of DS.

Conclusions: The privacy management architecture developed in this study enables the DS to dynamically manage information privacy in ubiquitous health and to define individual policies for all systems considering their trust value and corresponding attributes. The DS can also set policies for secondary use and reuse of health information. The architecture offers protection against privacy threats existing in ubiquitous environments. Although the architecture is targeted to ubiquitous health, it can easily be modified to other ubiquitous applications.

(JMIR Mhealth Uhealth 2013;1(2):e23) doi:10.2196/mhealth.2731

Original Paper

Privacy-Related Context Information for Ubiquitous Health

Antto Seppälä, MS Comp Sc; Pirkko Nykänen, PhD; Pekka Ruotsalainen, DSc (Tech)

Center for Information and Systems, School of Information Sciences, University of Tampere, Tampere, Finland

Corresponding Author:
Antto Seppälä, MS Comp Sc
Center for Information and Systems
School of Information Sciences
University of Tampere
Kanslerinrinne 1
Tampere, 33014
Finland
Phone: 358 407069919
Fax: 358 32191001
Email: Antto.Seppala@uta.fi

Abstract

Background: Ubiquitous health has been defined as a dynamic network of interconnected systems. A system is composed of one or more information systems, their stakeholders, and the environment. These systems offer health services to individuals and thus implement ubiquitous computing. Privacy is the key challenge for ubiquitous health because of autonomous processing, rich contextual metadata, lack of predefined trust among participants, and the business objectives. Additionally, regulations and policies of stakeholders may be unknown to the individual. Context-sensitive privacy policies are needed to regulate information processing.

Objective: Our goal was to analyze privacy-related context information and to define the corresponding components and their properties that support privacy management in ubiquitous health. These properties should describe the privacy issues of information processing. With components and their properties, individuals can define context-aware privacy policies and set their privacy preferences that can change in different information-processing situations.

Methods: Scenarios and user stories are used to analyze typical activities in ubiquitous health to identify main actors, goals, tasks, and stakeholders. Context arises from an activity and, therefore, we can determine different situations, services, and systems to identify properties for privacy-related context information in information-processing situations.

Results: Privacy-related context information components are situation, environment, individual, information technology system, service, and stakeholder. Combining our analyses and previously identified characteristics of ubiquitous health, more detailed properties for the components are defined. Properties define explicitly what context information for different components is needed to create context-aware privacy policies that can control, limit, and constrain information processing. With properties, we can define, for example, how data can be processed or how components are regulated or in what kind of environment data can be processed.

Conclusions: This study added to the vision of ubiquitous health by analyzing information processing from the viewpoint of an individual's privacy. We learned that health and wellness-related activities may happen in several environments and situations with multiple stakeholders, services, and systems. We have provided new knowledge regarding privacy-related context information and corresponding components by analyzing typical activities in ubiquitous health. With the identified components and their properties, individuals can define their personal preferences on information processing based on situational information, and privacy services can capture privacy-related context of the information-processing situation.

(JMIR Mhealth Uhealth 2014;2(1):e12) doi:10.2196/mhealth.3123

KEYWORDS

ubiquitous health; privacy; context information; trust; policy

Introduction

Overview

Ubiquitous computing makes it possible to collect all kinds of data anywhere and anytime [1] and allows integration of health care delivery and services into people's everyday lives [2,3]. This paper builds on a conceptual framework [4] in which ubiquitous health is defined as an open and dynamic ubiquitous information space. The space is presented as digital systems that consist of one or more information systems, their stakeholders, and environments. These systems create a dynamic network that offers and provides services to citizens. In the information space, individuals and service providers can select, tailor, and combine services and systems that belong to the network. To enable access to personal information, individuals and providers need to discuss trust, privacy level, and proffered service.

Ubiquitous health services can be offered by providers that are licensed and regulated by medical ethical codes and health care–specific legislation and other juridical norms and by actors that are not affected by health care–related regulations. To separate these two groups, we divided them as regulated health care services and other services. Providers offering regulated health care services have strict defined responsibilities and obligations concerning service provision, care, professionals, documentation, and information processing. There are also general regulations on privacy and security requirements (eg, data protection and processing directives) and business domain–specific regulations. Regulations cover laws; norms; good practice guidelines; and other rules controlling, constraining, or limiting activity of participants. These regulations can affect ubiquitous health services but they often do not meet the challenges of technological innovations well.

In ubiquitous health, trustworthiness and privacy are key challenges [4-6]. There are privacy threats created by autonomous and hidden processing of information and rich contextual metadata. There is no predefined trust between participants, and the business objectives, needs, interests, and policies of stakeholders may be unknown to the individual [4]. Information in ubiquitous health is highly sensitive and confidential, and the existence of services and actors that are not strictly regulated by health care-specific legislation creates threats and risks for individual privacy. In addition, information processing can happen in multiple systems and situations with different regulations, and risks of secondary use exist. The lack of predefined trust and privacy risks emphasizes the importance of an individual's ability to control his or her privacy.

For trusted information processing in ubiquitous health, we follow the principles presented in Ruotsalainen et al [4] and according to them, an individual should have the right to verify dynamically the trustworthiness of the ubiquitous health network and any system that requires or processes the individual's personal information for secondary purposes; control personal health information processing, inside systems and between them; be notified of all situations and contexts in which personal information is collected, processed, stored, and/or disclosed; and create situation-specific, context-aware, and granular personal privacy and trust policies, which control how personal information is collected, processed, disclosed, shared, stored, or destroyed.

Systems and stakeholders should have the responsibility to ensure trust verification by publishing their privacy policies and environmental and contextual features; openness of interests, business needs, and policies as well as their relationships with other systems; and transparency of information processing.

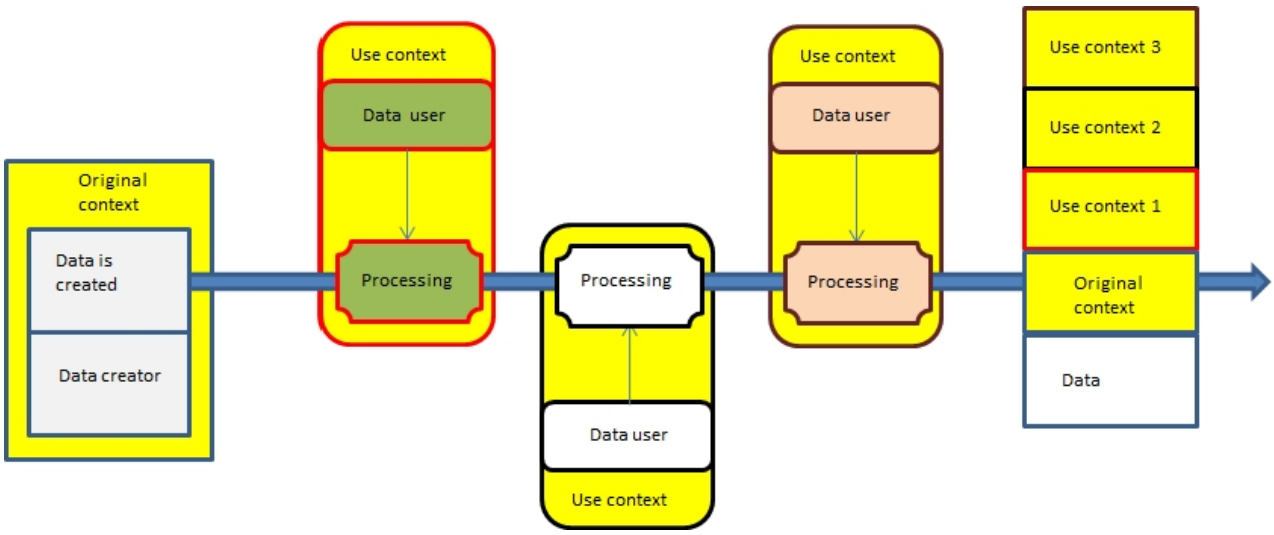
To protect his or her rights, an individual needs information about privacy, that is, privacy attributes, to define his or her personal privacy preferences. Privacy attributes enable privacy to be a concrete issue for individuals. In Nykänen et al [7], we defined privacy attributes as benefit, benevolence, capability, competence, confidence, context, reliability, and value. Privacy attributes and their contents have not generally been researched widely. The focus in this study is the context attribute, which refers to the situation in which data are created or processed. The objective is to analyze and define privacy-related context information components and their corresponding properties.

When data are created, a continuum of data is born. During the different processing situations, data or its properties may change. Original context refers to a situation when data are created. In various use contexts and processing situations, context information is incrementally created and it describes the current context and enables tracking of the context history. Thus, data have embedded context information that can be used by privacy services for trust calculation and to decide whether processing is allowed (Figure 1).

An individual's privacy preferences can be implemented with adaptable privacy policies. In previous work [8], we concluded a formula for privacy policies to contain (1) trust information that is a value of a system- or environment-specific calculation of regulatory compliance and trustworthiness; (2) sensitivity of the data; (3) situation of the information use; and (4) purpose of the data collection or use.

Policy formulation is a decision process in which an individual selects privacy rules and services and how much information can be traded compared to the offered service and the level of privacy attributes. In this study, our hypothesis is that context information enables formulation of context-aware privacy policies hence enabling trustworthy processing of personal health and wellness information and realizing individuals' rights for privacy in ubiquitous health. In Ruotsalainen et al [8], we presented a privacy architecture that could use context information in trust calculation and in context-aware privacy policies to control an individual's personal information. With this study, we add knowledge to our earlier research by studying the privacy-related context information and by defining the corresponding components and their properties that support privacy management in ubiquitous health.

Figure 1. Data continuum and context information.



Prior Work

Privacy and Trust

Privacy refers to an individual's ability to control information about him- or herself [9]. Privacy is a very personal concept and dependent on the context, because it may vary among jurisdictions, cultures, economies, time, and individuals [10-12]. Smith et al [13] claim that privacy is so bound to the specific context that it cannot be conceptualized as a single and unambiguous concept; rather it should be treated as a set of interests. Clarke [14] argues that it is useful to understand privacy as the interest of keeping personal space free from inference and has divided privacy into four dimensions: person, personal behavior, personal communications, and personal data. Information privacy means that personal information should not generally be available to other persons or organizations and an individual should have major control or influence over the personal data controlled by others and its use [14]. In this research, we refer to privacy as an individual's personal view within the legislative boundaries.

Trust is a concept closely related to privacy, and usually, the higher the value of trust, the lower the need for privacy [4]. Trust implicates the willingness to share personal information with others [15]. Schoorman et al [16] emphasize that trust is based on a relationship and the level of trust expresses the level of risk an individual is willing to take. Abdul-Rahman and Hailes [17] have defined three characteristics of trust: (1) trust is subjective, (2) actions we cannot monitor affect trust, and (3) trust level is dependent on how others' actions affect our actions. Several trust models has been developed for calculating trustworthiness [16,18-20].

Ubiquitous computing systems should be open and dynamic, because pre-identification of participants is impossible and they might change regularly [21]. In these kinds of distributed environments, collaboration is vital because multiple systems together try to achieve goals and perform tasks and it is crucial for systems to know which entities they should or should not interact with [22]. Traditional privacy and security solutions are not adequate for ubiquitous environments because there is no central control or predefined users or policies [19,21,23]. Privacy and security architecture and decisions need to be based on trust and its properties [19,21,24].

Context and Context Awareness

Context has been mostly defined with user profile, user emotion, and user location and identities of nearby people and objects and changes to those objects [25-28]. According to Dey et al [29], the three most relevant entities are places, people, and things. These entities have to be considered from different viewpoints such as location, activity, and identity. Dourish [30] proposes that context and content cannot be separated; the context arises from the activity itself and it cannot be an external description of the setting. He claims that context is a relational, interactional property between objects and activities and the scope of features must be defined dynamically [30]. Dey and Abowd ([28], pp. 3-4) defined context as: "Context is any information that can be used to characterize the situation of an entity. An entity is an individual, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves."

This definition is open and it considers that any information that is relevant for information processing in a situation can be used as a context. Context information can, for example, be information about the user, device, environment, or situation. Thus, it is meaningful to talk about context related to something that exists. There are three main uses for context information [29]: (1) presenting information and services to a user or using context to propose actions to be performed, (2) execution of a service automatically on behalf of the user, and (3) applications can tag context to information for later retrieval.

In context-aware computing, applications and systems are able to perceive their surroundings and environment, adapt according to the context, and perform autonomously. Context awareness refers to adaptability, which means that applications and systems exploit perceived context information and adapt their behavior accordingly [31]. In this view, context information is information that enables behavior modification based on this information and its relations. The systems, applications, and entities have to define the scope themselves.

According to Viswanathan et al [32], the key point for successful ubiquitous health is context awareness, and there are already several context-aware applications in the health and wellness domain. A lot of research has been done to support personalized actions and services in home care, chronic disease management, and ambient assisted living [33-37] with different personalized health status, body sensor networks, activity or behavior monitoring, decision support, and reminder applications [32,33,35-40]. In the hospital environment, many professionals are very agile, and context-aware technologies may help by personalizing services for them by location, time, and social context [41]. According to previous studies [33,42], there are several experiments on context-aware computing that have been created in hospital environments to improve patient record management, communication among professionals, and information sharing by including context awareness in patient room equipment.

Policies

In ubiquitous environments, privacy requirements can be expressed with policies. Privacy policy can be understood as a personal statement on privacy. With policies, individuals can set computational rules explicitly stating their personal privacy preferences on how their information can be processed, used, disclosed, and shared [21,43,44]. Policies are typically expressed with a policy language [45]. To enable personal privacy policies with computational rules requires definition of privacy attributes. Privacy policies can be implemented with setting values on privacy attributes. Context-aware policies based on context information enable dynamic adaptation of privacy control strategies and tailored privacy decision support services. A technique called sticky policy enables attaching policies into data to ensure that data are processed according to an individual's wishes [44].

Behrooz and Devlic [46] propose a context-aware privacy policy language based on two design considerations: (1) situations and privacy rules are defined separately, and (2) a context requestor can be specified based on its identity or social relationship to a user. These principles mean that privacy policies are set for different situations. Ghosh et al [47] presented a semantically rich policy-based system that can reason on user's context and thus protects a user's privacy dynamically during runtime. Schaub et al [23] presented a privacy context model with three major entities—user, user's environment, and user's activities. Their model takes into account information, physical, and territorial aspects of privacy. Blount et al [48] proposed a context-dependent policy model in which field context contains information when conditions for the policy are valid. These values may be from either the subject or the requestor.

Methods

Scenarios and User Stories

Scenarios are means to describe the system's intended usage. Scenario-based design techniques produce descriptions of how people do things and how they can accomplish different tasks with the system. With scenarios, designers can find new ways of doing things and new things to do. Scenarios capture goals, entities, behavioral information (eg, actions, activities, and events) and what people are trying to accomplish with the system [49,50]. They can also describe different related actors with their own objectives. Typically, scenarios have a plot that consists of several events, things that happen during activities, changes in the setting, etc. Scenarios are work-oriented analysis methods; thus, they are suitable for our purposes, because we are analyzing typical activities of an individual in an ubiquitous health environment to recognize the needs for context information.

In our previous articles, we analyzed privacy threats and the principles for trusted information processing [4], defined privacy attributes [7], and analyzed the requirements for information that should be used in privacy policy formulation and common threats and challenges concerning privacy in ubiquitous health [8]. Our previous results created the framework for the scenario development and analyses and for the requirements for context information. In this research, we created scenarios that were based on materials collected in our earlier empirical research on personal wellness [51-53] performed with focus groups and literature studies focusing on health and wellness activities and technical applications on chronic disease management, self-health management, ubiquitous health, and wellness approaches. Scenarios were designed to capture the characteristics of different situations, such as a general wellness management situation without any specific needs and a specific setting with a chronic disease. With scenarios, we could identify a wide selection of typical activities in ubiquitous health.

We first created two textual scenarios describing the main actors, their backgrounds, and current health and wellness situations and next, we determined the main goals, activities, and entities. Then, we further divided both scenarios into 10 user stories that described in more detail the activities and services the individuals needed in their situations. Each user story focuses on 1 activity of a scenario and it is a short textual and informal description of a user case. Because context arises from activity [30] with the user stories, we could capture activities in ubiquitous health to identify information-processing situations and privacy-related context information.

At first, scenarios described typical wellness approaches emphasizing services that are not regulated by health care regulations, for example, lifestyle management and health-related behaviors. The objective was to recognize activities and entities outside regulated health care services. Then we approached chronic disease management scenarios with a focus on identifying collaboration between regulated health care services and personal attempts to manage health outside the provider networks with other services. These scenarios were analyzed to recognize activities and information-processing situations. To summarize, these scenarios helped us to analyze the aspects of two different situations in ubiquitous health: (1) ubiquitous health without regulated health care providers' participation; and (2) ubiquitous health with regulated health care, for example, service portfolio is a combination of services produced by a regulated health care provider(s) and other health and wellness providers.

An Example Scenario

As an example, we present the following scenario. Peter is a 23-year-old healthy student who begins to feel tired and ill and he decides to seek help from student health services. After a few tests and doctor visits, Peter is diagnosed with type 2 diabetes mellitus. From now on, Peter has to pay attention to his habits and choices concerning healthy living for the first time in his life. We divided this scenario into more detailed user stories describing activities related to chronic diseases in a ubiquitous health environment. In Table 1, we present an example analysis of a user story. In Table 2, we present a detailed example of a single activity in ubiquitous health with its related privacy concerns, Peter's policies, and the context information that a policy example requires.

Table 1. An example analysis of a user story in chronic disease scenario. User story 2.1: Peter receives a medical device with sensors to manage and care for his disease and automatically measure and monitor his condition. Devices can also automatically inform his doctor about the results and major changes.

Role	Individual and information controller with rights for privacy, to control processing and secondary use of information. Peter can decide who can access data created by the device. Peter needs privacy policies to control his own personal health system (PHS) use and the information it contains.
Activities	Data is created in the sensors and transferred to PHS. PHS analyzes the information and compares it to past information. PHS informs Peter's doctor about a major change in a value. Doctor accesses the information and makes a medical decision.
Environment	Anywhere. No health care–specific regulations concerning the environment. Information sharing is based on Peter's known consent and privacy policies. All information created by the certified device is trusted. The device is regulated by specific legislation (eg, the European Union directive on medical devices). In case of a major change in measurement information, regulated health care service will participate and then the environment will be strictly regulated by health care–specific regulations.
Information systems	Medical device, Peter's own PHS and possibly electronic health record system. Sensor and measurement data is stored in PHS and Peter's health records are in regulated electronic health record system. Peter has total control over his PHS.
Stakeholders	Peter, medical device, PHS, and licensed medical professional (doctor) with responsibilities concerning care and patients privacy
Services	Certified medical device measuring blood sugar levels PHS diabetic information analysis Regulated health care service activated by Peter's PHS in case of a major change in Peter's measurement values
Information content	Measurement and monitoring data from sensors and medical device Health and wellness information in PHS is controlled by Peter. The medical information is regulated in health care organization's electronic health record system.
Original context of the information	Information is created by a certified medical device controlled by Peter. The environment does not have any specific domain regulations. Information is in Peter's control and he has full rights for it. Peter's personal context-aware privacy policies are the main source for limitations and constraints on information processing.
Requirements for context properties	Peter's PHS is a trusted information system in his control so it has full processing rights and can activate other services if needed following Peter's privacy policies. Peter has defined in his policies that different measurement and sensor data is very sensitive and sets limitation for what purpose information can be used. In other cases, PHS cannot grant access to information without Peter's authorization. Other than regulated health care, services have to share their principles for information processing, security and privacy policies, and for what purpose they want to process the information.

Table 2. An example analysis of an activity: data is created in the sensors and transferred to the PHS.

Privacy challenges and threats [8]	Peter's policies	Required context information for policy 1
Lack of awareness	1. Peter thinks that this kind of data is highly personal and can only be accessed automatically by a health care professional participating in Peter's care service.	Situation: activity, processing type, actor, target, information sensitivity, and purpose for processing
It is difficult to know how data is used in the future	2. To use the data, transparency of processing is needed; therefore, the provider has to publish detailed privacy and security policies and allow third-party auditing.	Environment: general privacy and security regulations, location, and society
Relationships between systems may be unknown	3. To prevent secondary use, copying data is not allowed. If copying is required, Peter has to be notified and his known consent is required.	Service: type, role, provider, location, and objective
Potential secondary use of information	4. Health care professionals are not allowed to disclose data without Peter's known consent.	Individual: role, rights to control information, relation to the activity, confidentiality requirements
Users want to control how systems use personal health information		Stakeholder: identity, type, role, purpose, and justification for processing
How to guarantee that data is processed following the legal constraints and according to the individual's policies		IT system: identity, type, controller

Results

In an open and dynamic ubiquitous health information space, there are no possibilities to predefine entities or activities and most aspects of information processing are dynamic. In the scenarios and user story analyses, we recognized how different activities are reasons for information-processing situations in ubiquitous health, how several entities can create and use information, and how the same information can be used later to support different activities. In addition, scenarios showed that activities could happen autonomously with information systems even without human participation; for instance, based on some measurement of vital signs or monitoring of data. Thus, information processing happens because some entity performs an activity in a certain environment. Situation describes this occurrence and therefore is chosen as the core component defining privacy-related context information. It is linked to a certain activity; that is, the reason for information processing. Context information needs to include the whole situation and all participants because of the dynamic nature and limitations in predefining activities and stakeholders in ubiquitous health.

As a result of our scenarios and user stories, we present the two kinds of basic models for ubiquitous health: ubiquitous health without regulated health care providers, and ubiquitous health with regulated health care service providers.

The first case is an open environment with multiple entities with different kinds of domain environments and interests. All participants are by definition untrusted. Health care–specific regulations do not apply, but regular privacy and security legislations set limitations for information processing. In addition, different domains may have their specific legislations (eg, social care, wellness services, medical devices, or pharmacy). Environment and entity-specific regulations and an individual's personal context with privacy preferences are necessary for adaptable privacy policies. An individual's role, environment, and privacy requirements may vary between used services or information systems and information sensitivity influences heavily on personal policies. An individual's rights to control data and information must be discussed with service providers.

In the second case, there are also entities that are affected by health care–specific regulations. Depending on who or what provides service and/or controls information, there might be strict health care–specific regulations for service provision, organizations, professionals, information systems, and information processing. Regulated health care services are to some extent trusted and privacy threats and risks occur especially when information is transferred from them or processed beyond their authority. It is very critical to capture who is responsible for what, where and how services are provided, what information and sources are used, how sensitive the information is, and who controls participating information systems.

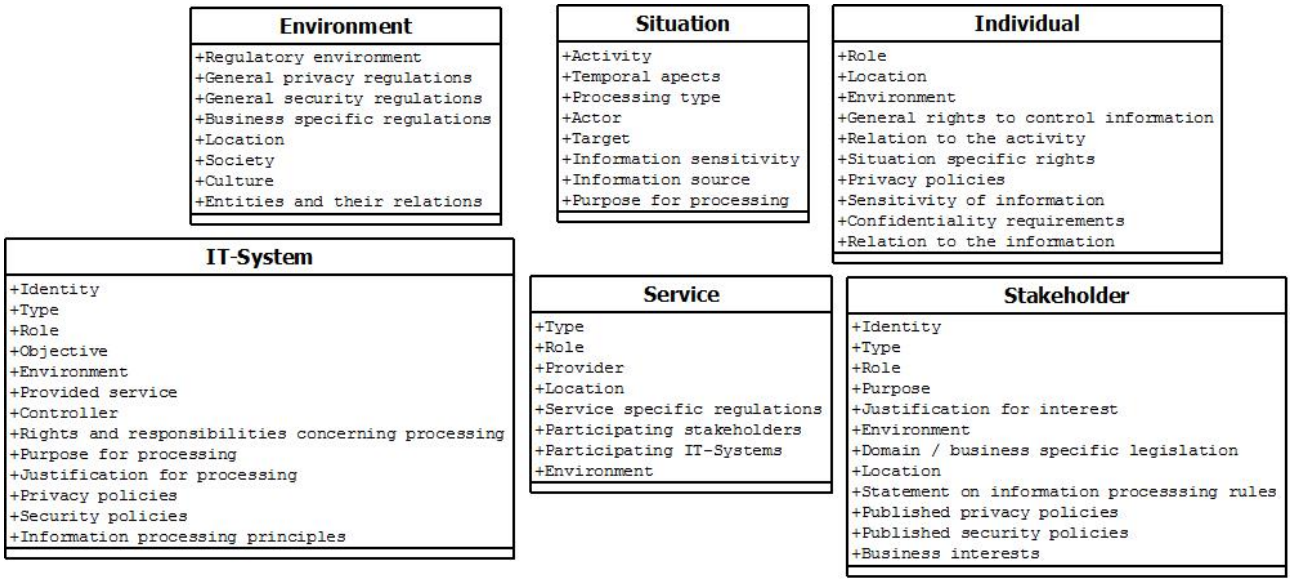
In a previous study [4], we defined ubiquitous health to be composed of services, information systems, stakeholders, and their environments. In addition to these, we have to capture the contexts of the information-processing situation and its object and/or subject. We should capture the following components and their properties on privacy, regulations, and requirements for trusted information processing: what happens (situation); who is the subject or the object (individual); what services are related to the situation (service); where this situation happens (environment); what social actors are active in the situation (stakeholder); and what computational entities participate (IT system).

In this research, the properties of the privacy-related context information components and their properties are derived by combining the results of the scenario analyses and the principles and requirements presented in the earlier research. We analyzed the results of the scenario analyses to explicate concrete properties for our components. In the example, we derived the context information that is needed to fulfil the requirements for

policies and to minimize known privacy threats. In this example, policy 1 in the Table 2 means that Peter sets a general policy that data created by sensors is highly sensitive and can only be automatically accessed by health care professionals participating in his care. Peter has total control over his data and the future use of data is based solely on Peter's wishes. The situation occurs when a regulated health care professional tries to access Peter's data to support Peter's care and to follow his condition. To manage his privacy, Peter needs information about the data user's environment and processing wishes. If parties other than a health care professional in Finland taking part in Peter's care service want to access the data, Peter's known consent is required. The data user is a regulated health care professional in Finland; that is, predefined as somewhat trusted and he/she can use the information only to make medical decisions and to follow Peter's condition. The data can only be accessed within Peter's PHS and the data cannot be copied or distributed. From the example, we can see how Peter needs several kinds of context information to create the example policy.

From the scenario analyses, we have defined the properties that are needed to fulfil the principles of trusted information processing and requirements set for privacy formulation concerning context information (Figure 2).

Figure 2. Privacy-related context information components and their properties for ubiquitous health.



A situation describes information processing that happens in a certain context because of some activity and by/for a certain individual. From the scenarios, we learned that environments might vary a lot; therefore, we need to understand the environment where the situation happens and component-specific environments (eg, individual, services, stakeholders, and IT systems) to capture all privacy aspects. With the environment, we do not only mean location and other position-based information, but especially important is to capture the type of environment. We have to perceive the properties of environment such as privacy, security, trust-related information, and information-processing rules and responsibilities. Regulations may differ a lot between environments and different businesses are affected by their specific legislation. Capturing environment is crucial because technological advancements such as cloud computing and big data create new types of privacy risks. For example, if a service is offered in the European Union but the data are stored or processed in an information system located in the United States, there are differences in legislations concerning privacy, security, or secondary use of data. People should be able to control where and why their data are processed.

An individual component describes the actual subject and/or object of health and wellness activities in ubiquitous health. It is linked differently to situations; an individual can create them, participate in them, and/or is an object. Properties needed from the individual are the role he/she has in the situation, location, and environment and what relation he/she has with the activity. Also, an individual's rights for controlling information processing (eg, content, disclosure and access to information), privacy policies, sensitivity and confidentiality requirements and what is his/her relation (eg, owner, controller, or subject) to information should be acknowledged. All these things affect how and on what basis systems can process information.

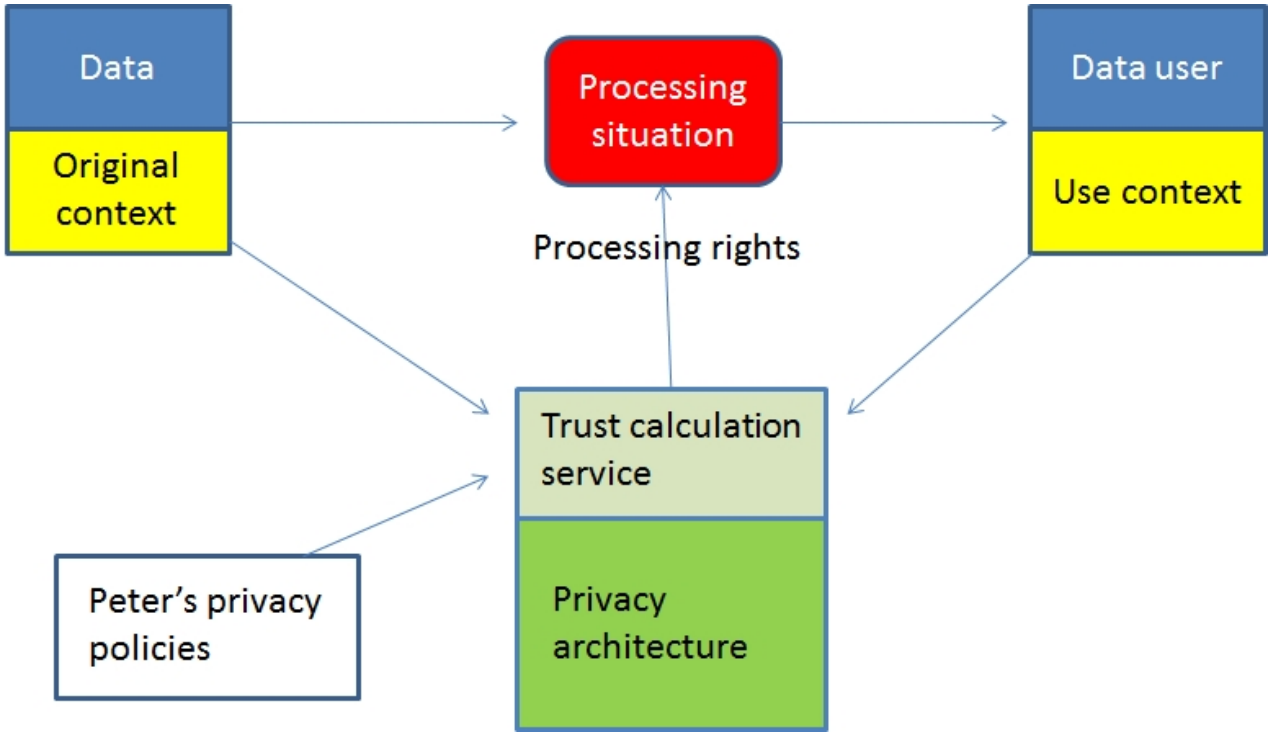
A service component describes regulated health care services and/or other services that can be offered by IT systems and/or stakeholders. An IT system component refers to all computational entities, which can include health information systems, personal health systems, ubiquitous systems, devices, sensors, etc. IT systems should be open about their processes and publish their privacy and security policies including how an individual's privacy is protected, relevancy of processing and actual data protection specifications, and detailed information-processing principles. This would improve transparency of information processing and increase trustworthiness. If an IT system does not publish necessary information, this has to be captured in the context information. Because information processing can happen anywhere, it is vital to capture its context because there are several characteristics affecting privacy that may differ between IT systems; for example, type, location, or regulative background. For example, there are big differences in regulations among information

systems, regulated medical devices (eg, have to be certified), and wellness devices. Stakeholder is the social component describing organizations and possible human participants. They can be actors or interested parties in a situation. They offer, participate, or are interested in services offered to individuals.

Our components can be used to increase trustworthiness of information processing because privacy policies can be adaptable and based on constraints, limitations, rules, rights, and responsibilities set with situational information. Components can also be used to analyze that the information processing follows the preferences set by an individual's privacy policies and the requirements from the original context of the information. For example, in our user story Peter may disclose medical and lifestyle data to a service provider to receive a selected service. Peter has set privacy policies using privacy properties. Before disclosure, Peter (his privacy architecture) needs the context information from the service provider to calculate if processing is according to the requirements set by Peter's own context-aware privacy policies and the original context of the information. Privacy architecture can then confirm that the use context is valid according to Peter's personal preferences and allow access to the information (Figure 3).

Our hypothesis was that privacy-related context information could be used to formulate context-aware privacy policies hence enabling trusted processing of personal health and wellness information. In this study, we analyzed contents of a privacy attribute context and presented components and their properties that can be used as part of privacy policies by setting situational constraints and limitations. These characteristics are also needed to capture information-processing contexts from the privacy perspective. All components or properties are not necessarily needed in all situations. In addition, if some systems refuse to cooperate in publishing context information, this has to be captured and acknowledged.

Figure 3. The use of privacy-related context information in ubiquitous health.



Discussion

In this research, we present an approach using privacy-related context information for privacy protection in ubiquitous health. Privacy is a business-enabler because individuals will not use these services if they cannot manage their privacy and trust. People need simple tools to manage their privacy and we have started this by defining the components situation, environment, individual, service, stakeholder, IT system, and their properties. These components describe the crucial privacy-related context information needed to improve trustworthiness of ubiquitous health. We present new knowledge by defining context, which is one of the main privacy attributes used in privacy policy definition. The results of this study can be used as a basis to create more formal models defining privacy-related context information in a computer-understandable format. Our results are in line with the preferred privacy level model by Lederer et al [11] but we have taken it a step further and divided context into original and use context and defined more detailed and concrete properties that could be valued and measured and used by privacy architecture for trust calculation.

Ubiquitous health is still an emerging field combining highly regulated health care with personal health and wellness services and systems. In health care, legislation and regulations define what privacy is and what kind of rights individuals have; that is, privacy is a state-defined property. Considering services and systems outside the regulated health care privacy is a personal property of an individual; that is, free will. The individual has the right to choose the use of his/her information and define policies as to how, where, and to what extent the information can be processed. In ubiquitous health, a privacy model is a combination of these two models and can be controlled with

policies. Policies can be personal preferences or defined by regulations. Using the scenarios, we could identify situations outside regulated health care to recognize requirements and characteristics of ubiquitous health. With organization-centric health care processes or workflows, we cannot really model ubiquitous health as a whole because there are many services and systems without predefined and regulated processes or workflows.

In ubiquitous health, service provision is based on customer relationships and trading on benefits of services against reducing personal privacy. Individuals should be able to verify the trustworthiness of service providers and decide if they are prepared to disclose personal information and reduce privacy. Because services are often offered as distributed, personalized and even autonomous, the privacy architecture should offer automatic privacy services and adapt dynamically to the situation. Scenarios and user stories showed that ubiquitous health is multidimensional with limitations of predefining situations. The amount of information needed and created in these situations can be huge, and the content and its sensitivity vary depending on the activity performed. Ubiquitous health is an open, dynamic, and collaborative environment and privacy needs to be based on trust and its properties [19,21,24].

In health care, privacy is mainly protected with access control and consent management. Access control is merely one tool to protect privacy. Managing privacy in ubiquitous health is a much broader issue than just controlling health care professionals' access to data. Access control with predefined rights, roles, and consents cannot really function because there is no central control or necessarily predefined processes, situations, or actors. To ensure privacy in ubiquitous computing, access control should be dynamic because of multiple changing entities. Context information enables dynamic management of rights [54]. Consent is an example of a personal policy but in ubiquitous health, policies are needed to cover several different situations that are more complex than those that consents are designed for. Policies have to be dynamic and context-aware. Corradi et al [55] present a dynamic and flexible security middleware that uses context as a basic concept in security policy specification and permissions are linked to the contexts instead of user identities or roles. Most research on privacy of context-aware computing focuses on capturing user's context or certain actors and using that information to adapt to privacy preferences [23,47,54].

In this study, we followed the approach of Behrooz and Devlic [46] to separate situations and privacy rules. We identified the necessary information to capture privacy aspects in information-processing situations. Then, privacy architecture can capture the situation and the conditions where data are created; that is, the original context and combine that with individual's policies and control future use contexts such as how, where, and by whom the information can be used. Our approach needs information from participating systems and currently its availability depends on the goodwill of participants. Additional to this information, privacy architecture can use external sources for estimating trustworthiness of systems (eg, recommendations from others, history, trust values, and trust calculations).

In the European Union, organizations are required to inform individuals about use of their data and publish privacy policies that should be comprehensive with high-level descriptions of their privacy practices [43]; however, these are not enough to safeguard individuals' rights. These privacy policies do not generally consider how data are actually processed after collection. So, one of the main challenges in privacy protection is how to enforce all relevant parties to explicate their detailed privacy policies [43]. Current legislation is not fully prepared to handle privacy threats of ubiquitous computing and does not obligate organizations to disclose their detailed privacy policies or information-processing principles. In the future, legislation needs to include the needs of privacy, citizens' rights, and ubiquitous computing. Citizens have to be able to control processing and secondary use of their personal information. Future privacy principles and norms need to progress from high-level principles to detailed regulations concerning the processing and use of information. This would bring openness and transparency to information processing and new kinds of responsibilities for organizations and informed rights for citizens. In addition, authorities or certificate organizations should be able to audit providers and offer recommendations about their trustworthiness.

The components defined in this research may have some limitations and may not be conclusive; however, based on the scenario analyses these are needed. In addition, some properties are hard to define explicitly or in measurable format. They have to be analyzed in more detail and formal models are needed to implement them in computational format. Also, we need more detailed analysis of what organizations should publish about their processes and privacy and security policies and principles. To create context-aware privacy services and policies in practice, we need to develop ontologies that explicate components, properties, and requirements that we have presented in this research. Ontologies are formal representations and should cover different activities, services, IT systems, stakeholders, information content, and especially relevant regulative environments. With ontologies, we can create computational rules that can be used to enforce regulations and personal policies into ubiquitous applications.

Because it is practically impossible for individuals to evaluate the trustworthiness of a system, and to understand detailed privacy and security requirements and set personal policies, we developed trust-based privacy management architecture for ubiquitous health [8]. This architecture model describes what privacy and security services are needed to enable trusted information processing in ubiquitous health. The architecture will apply privacy-related context information to create privacy and security policies that will ensure that information processing will not happen against the wishes of the individual and the original context of the data. The architecture contains decision support and policy services for individuals to help them define personal policies. This research adds to the architecture model by defining the required privacy-related context information components and their properties that are needed to create implementable tools and means for individuals to manage personal information privacy.

Acknowledgments

We acknowledge funding of the Trusted eHealth and eWelfare Space (THEWS) research project by the Finnish Academy of Sciences in the MOTIVE Research Programme during 2009–2012. The first author acknowledges the support of the Tampere Doctoral Programme in Information Science and Engineering (TISE).

Conflicts of Interest

None declared.

References

1. Varshney U. Pervasive healthcare and wireless health monitoring. Mobile Netw Appl 2007 Jul 12;12(2-3):113-127. [doi: 10.1007/s11036-007-0017-1]
2. Korhonen I, Bardram JE. Guest editorial: introduction to the special section on pervasive healthcare. IEEE Trans Inf Technol Biomed 2004 Sep;8(3):229-234. [Medline: 15484426]
3. Arnrich B, Mayora O, Bardram J, Tröster G. Pervasive healthcare: paving the way for a pervasive, user-centered and preventive healthcare model. Methods Inf Med 2010;49(1):67-73. [doi: 10.3414/ME09-02-0044] [Medline: 20011810]
4. Ruotsalainen PS, Blobel BG, Seppälä AV, Sorvari HO, Nykänen PA. A conceptual framework and principles for trusted pervasive health. J Med Internet Res 2012;14(2):e52 [FREE Full text] [doi: 10.2196/jmir.1972] [Medline: 22481297]
5. Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. ACM Comput. Surv 2012 Nov 01;45(1):1-54. [doi: 10.1145/2379776.2379779]
6. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 2012 Feb;36(1):93-101 [FREE Full text] [doi: 10.1007/s10916-010-9449-4] [Medline: 20703745]
7. Nykänen P, Seppälä A, Ruotsalainen P, Blobel B. Feasibility analysis of the privacy attributes of the personal wellness information model. Stud Health Technol Inform 2013;192:219-223. [Medline: 23920548]
8. Ruotsalainen PS, Blobel B, Seppälä A, Nykänen P. Trust Information-Based Privacy Architecture for Ubiquitous Health. J Med Internet Res 2013 Oct 08;1(2):e23. [doi: 10.2196/mhealth.2731]
9. Belanger F, Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly 2011;35(4):1017-1041.
10. Westin AF. Social and political dimensions of privacy. J Social Issues 2003 Jun;59(2):431-453. [doi: 10.1111/1540-4560.00072]
11. Lederer S, Deay AK, Mankoff J. A conceptual model and metaphor of everyday privacy in ubiquitous computing environments. UCB/CSD-2-1188, UC Berkeley College of Engineering Technical Reports. Berkeley, CA: Computer Science Division, University of California; 2002. URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2002/CSD-02-1188.pdf [accessed 2013-11-19] [WebCite Cache ID 1384860048852087]
12. Skinner G, Song H, Chang E. Defining and protecting meta privacy: a new conceptual framework within information privacy. 2006 Presented at: 22nd International Conference on Data Engineering Workshops; April 3-7, 2006; Atlanta, GA, USA. [doi: 10.1109/ICDEW.2006.46]
13. Smith JH, Dinev T, Xu H. Information privacy research - an interdisciplinary review. MIS Quarterly 2011;35(4):989-1016.
14. Clarke R. Internet privacy concerns confirm the case for intervention. Commun ACM 1999;42(2):60-67. [doi: 10.1145/293411.293475]
15. Pavlou PA. State of the information privacy literature: where are we now and where should we go? MIS Quarterly 2011;35(4):977-988.
16. Schoorman FD, Mayer RC, Davis JH. An integrative model of organizational trust: past, present, future. Academy of Management Review 2007 Apr 01;32(2):344-354. [doi: 10.5465/AMR.2007.24348410]
17. Abdul-Rahman A, Hailes S. A distributed trust model. In: New Security Paradigms Workshop: Proceedings, September 23-27, 1997, Langdale, Cumbria, United Kingdom. New York: Association for Computing Machinery; 1998.
18. Lu G, Lu J, Yao S, Yip J. A review on computational trust models for multi-agent systems. TOISCIJ 2009 Mar 19;2(2):18-25. [doi: 10.2174/1874947X00902020018]
19. Khiabani H, Sidek ZM, Manan JA. Towards a unified trust model in pervasive systems. In: 24th IEEE International Conference on Advanced Information Networking and Applications Workshops. Piscataway, NJ: The Institute of Electrical and Electronics Engineers, Inc; 2010 Presented at: Advanced Information Networking and Applications Workshops (WAINA), IEEE 24th International Conference on; 20-23 April 2010; Perth, WA p. 831-835. [doi: 10.1109/WAINA.2010.144]
20. Krukow K, Nielsen M, Sassone V. Trust models in ubiquitous computing. Philos Trans A Math Phys Eng Sci 2008 Oct 28;366(1881):3781-3793. [doi: 10.1098/rsta.2008.0134] [Medline: 18678555]
21. Joshi A, Finin T, Kagal L, Parker J, Patwardhan A. Security policies and trust in ubiquitous computing. Philos Trans A Math Phys Eng Sci 2008 Oct 28;366(1881):3769-3780. [doi: 10.1098/rsta.2008.0142] [Medline: 18672450]

22. Uddin GM, Zulkernine M, Ahamed SI. CAT: a context-aware trust model for open and dynamic systems. In: SAC '08 Proceedings of the 2008 ACM Symposium on Applied Computing. New York: ACM; 2008 Presented at: The ACM symposium on Applied computing; March 16-20, 2008; Brazil p. 2024-2029. [doi: 10.1145/1363686.1364176]
23. Schaub F, Koenings B, Dietzel S, Weber M, Kargl F. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, UbiComp 2012, CASEMANS 2012 Workshop. New York: ACM; 2012 Presented at: The ACM Conference on Ubiquitous Computing, UbiComp , CASEMANS Workshop; September 8, 2012; Pittsburgh, PA, USA p. 752-757. [doi: 10.1145/2370216.2370383]
24. Ruohomaa S, Kutvonen L. Trust management survey. Heidelberg: Springer; 2005 Presented at: Trust Management: Third International Conference, iTrust 2005; May 23-26, 2005; Paris, France p. 77-92. [doi: 10.1007/11429760_6]
25. Fitrianie S, Tatomir I, Rothkrantz L. A context aware and user tailored multimodal information generation in a multimodal HCI framework. : Eurosis; 2008 Presented at: EUROMEDIA; 2008; Ghent, Belgium p. 95-103.
26. Addas S. A call for engaging context in HCI/MIS-research with examples from the area of technology interruptions. AIS Transactions in Human-Computer Interaction 2010;2(4):178-196.
27. Johns G. In praise of context. J Organiz Behav 2001 Feb;22(1):31-42. [doi: 10.1002/job.80]
28. Dey AK, Abowd GD. Towards a better understanding of context and context-awareness.: GVU Technical Report; GIT-GVU-99-22; 1999. URL: https://smartech.gatech.edu/bitstream/handle/1853/3389/99-22.pdf [accessed 2014-03-06] [WebCite Cache ID 6Nrnzdg2F]
29. Dey A, Abowd G, Salber D. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. Human-Comp Interaction 2001 Dec 1;16(2):97-166. [doi: 10.1207/S15327051HCI16234_02]
30. Dourish P. What we talk about when we talk about context. Personal and Ubiquitous Computing 2004 Feb 1;8(1):19-30. [doi: 10.1007/s00779-003-0253-8]
31. Soylu A, Causmaecker P, Desmet P. Context and adaptivity in pervasive computing environments: links with software engineering and ontological engineering. Journal of Software 2009 Nov;4(9):992-1013. [doi: 10.4304/jsw.4.9.921-1013]
32. Viswanathan H, Chen B, Pompili D. Research challenges in computation, communication, and context awareness for ubiquitous healthcare. IEEE Commun. Mag 2012 May;50(5):92-99. [doi: 10.1109/MCOM.2012.6194388]
33. Paganelli F, Giuli D. An ontology-based system for context-aware and configurable services to support home-based continuous care. IEEE Trans Inf Technol Biomed 2011 Mar;15(2):324-333. [doi: 10.1109/TITB.2010.2091649] [Medline: 21075729]
34. Paganelli F, Giuli D. An ontology-based context model for home health monitoring and alerting in chronic patient care networks. : IEEE Computer Society Press; 2007 Presented at: 21st International Conference on Advanced Networking and Applications Workshops/Symposia; 21-23 May, 2007; Niagara Falls, Ontario, Canada p. 838-845. [doi: 10.1109/AINAW.2007.90]
35. Catarinucci L, Colella R, Esposito A, Tarricone L, Zappatore M. RFID sensor-tags feeding a context-aware rule-based healthcare monitoring system. J Med Syst 2012 Dec;36(6):3435-3449. [doi: 10.1007/s10916-011-9794-y] [Medline: 22083369]
36. Fenza G, Furno D, Loia V. Hybrid approach for context-aware service discovery in healthcare domain. Journal of Computer and System Sciences 2012 Jul;78(4):1232-1247. [doi: 10.1016/j.jcss.2011.10.011]
37. Das B, Seelye AM, Thomas BL, Cook DJ, Holder LB, Schmitter-Edgecombe M. Using smart phones for context-aware prompting in smart environments. 2012 Presented at: Consumer Communications and Networking Conference (CCNC), IEEE; 14-17 Jan. 2012; Las Vegas, NV p. 399-403. [doi: 10.1109/CCNC.2012.6181023]
38. Wongpatikaseree K, Ikeda M, Buranarach M, Supnithi T, Lim AO, Yasuo T. Activity recognition using context-aware infrastructure ontology in smart home domain. In: Proceedings 2012 Seventh International Conference on Knowledge, Information and Creativity Support Systems. Piscataway, NJ: The Institute of Electrical and Electronics Engineers, Inc; 2012 Presented at: Knowledge, Information and Creativity Support Systems (KICSS) Seventh International Conference; 8-10 Nov, 2012; Melbourne, VIC p. 50-57. [doi: 10.1109/KICSS.2012.26]
39. Zhang D, Yu Z, Chin CY. Context-aware infrastructure for personalized healthcare. Stud Health Technol Inform 2005;117:154-163. [Medline: 16282665]
40. Peleg M, Broens T, González-Ferrer A, Shalom E. Architecture for a ubiquitous context-aware clinical guidance system for patients and care providers. Heidelberg: Springer-Verlag; 2013 Presented at: KR4HC'13 / ProHealth'13; 2013; Murcia, Spain p. 161-167.
41. Jahnke JH, Bychkov Y, Dahlem D, Kawasame L. CEUR Workshop Proceedings (Vol. 114). 2004. Implicit, context-aware computing for health care URL: http://www.ics.uci.edu/~lopes/bspc04-documents/Jahnke.pdf [accessed 2013-11-19] [WebCite Cache ID 1384864716838609]
42. Bricon-Souf N, Newman CR. Context awareness in health care: a review. Int J Med Inform 2007 Jan;76(1):2-12. [doi: 10.1016/j.ijmedinf.2006.01.003] [Medline: 16488663]
43. Guarda P, Zannone N. Towards the development of privacy-aware systems. Information and Software Technology 2009 Feb;51(2):337-350. [doi: 10.1016/j.infsof.2008.04.004]
44. Pearson S, Casassa-Mont M. Sticky Policies: An Approach for Managing Privacy across Multiple Parties. Computer 2011 Sep;44(9):60-68. [doi: 10.1109/MC.2011.225]

45. Chakraborty S, Ray I. p-Trust: a new model of trust to allow finer control over privacy in peer-to-peer framework. JCP 2007 Apr 01;2(2). [doi: 10.4304/jcp.2.2.13-24]
46. Behrooz A, Devlic A. A context-aware privacy policy language for controlling access to context information of mobile users. In: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin Heidelberg: Springer; 2012:25-39.
47. Ghosh D, Joshi A, Finin T, Jagtap P. Privacy control in smart phones using semantically rich reasoning and context modeling. In: SPW 2012 IEEE CS Security and Privacy Workshops. Piscataway, NJ: The Institute of Electrical and Electronics Engineers, Inc; 2012 Presented at: Security and Privacy Workshops (SPW), IEEE Symposium; May 24-25, 2012; San Francisco, CA p. 82-85. [doi: 10.1109/SPW.2012.27]
48. Blount M, Davis J, Ebling M, Jerome W, Leiba B, Xuan L, et al. Privacy engine for context-aware enterprise application services. 2008 Presented at: Embedded and Ubiquitous Computing, EUC '08. IEEE/IFIP International Conference on , vol.2; 17-20 Dec. 2008; Shanghai p. 94-100. [doi: 10.1109/EUC.2008.130]
49. Carroll J. Five reasons for scenario-based design. Interacting with Computers 2000 Sep;13(1):43-60. [doi: 10.1016/S0953-5438(00)00023-0]
50. Rolland C, Ben Achour C, Cauvet C, Ralyté J, Sutcliffe A, Maiden N, et al. A proposal for a scenario classification framework. Requirements Eng 1998 Mar;3(1):23-47. [doi: 10.1007/BF02802919]
51. Nykänen P, Seppälä A. Collaborative approach for sustainable citizen-centered health care. In: Wickramasinghe N, Bali RK, Suomi R, Kirn S, editors. Critical Issues for the Development of Sustainable E-health Solutions (Healthcare Delivery in the Information Age). New York: Springer; 2012:115-134.
52. Seppälä A, Nykänen P, Ruotsalainen P. Development of personal wellness information model for pervasive healthcare. Journal of Computer Networks and Communications 2012;2012:1-10. [doi: 10.1155/2012/596749]
53. Seppälä A, Nykänen P. Contextual analysis and modeling of personal wellness. 2011 Presented at: the International Conference Knowledge Engineering and Ontology Development; Oct 2011; Paris, France p. 202-207.
54. Faravelon A, Chollet S, Verdier C, Front A. Enforcing privacy as access control in a pervasive context. 2012 Presented at: Consumer Communications and Networking Conference (CCNC) IEEE; 14-17 Jan; Las Vegas, NV p. 380-384. [doi: 10.1109/CCNC.2012.6181011]
55. Corradi A, Montanari R, Tibaldi D. Context-based access control management in ubiquitous environments. In: Network Computing and Applications. Los Alamitos, CA: IEEE Computer Society; 2004 Presented at: Third IEEE International Symposium on Network Computing and Applications; August 30-September 1, 2004; Cambridge, MA p. 253-260. [doi: 10.1109/NCA.2004.1347784]

Abbreviations

IT: information technology
PHS: personal health system

Edited by G Eysenbach; submitted 21.11.13; peer-reviewed by S Koch, J Zvarova, S Mohammed; comments to author 16.12.13; revised version received 26.01.14; accepted 12.02.14; published 11.03.14

Please cite as:
Seppälä A, Nykänen P, Ruotsalainen P
Privacy-Related Context Information for Ubiquitous Health
JMIR Mhealth Uhealth 2014;2(1):e12
URL: http://mhealth.jmir.org/2014/1/e12/
doi:10.2196/mhealth.3123
PMID:

KEYWORDS

ubiquitous health; privacy; computational trust; policy; context-awareness

Introduction

Overview

Both ubiquitous health and pervasive health are terms that describe a new business model (these terms have been used in many papers synonymously). Similarly to health care, its goal is to make health services available to everyone, but many of its features separate it from health care [1]. According to Ruotsalainen et al, ubiquitous health is a metasystem that is a dynamic network of interconnected systems offering health services to a data subject (DS) in an unsecure information space [1]. Contrary to health care where the services are defined by health professionals, in ubiquitous health, the DS creates the network, selects the systems, and sets rules (policies) that regulate how and by whom the DS' health information is used and shared. In ubiquitous health, the existence of predefined trust between the DS and systems cannot be assumed, and systems' features, their business goals, and regulation systems followed are often unknown. Furthermore, health care-specific regulations do not rule the ways health data is processed and shared [1]. It is evident that ubiquitous health features generate privacy and trustworthiness challenges that should be solved to make it successful.

Privacy is a complex, personal, and situation-depending concept that can be interpreted in various ways [2]. Westin defined privacy as "the claim of an individual to determine what information about himself or herself should be known to others and what uses will be made of it by others" [3]. Privacy is also a human right that is protected by international directives and constitutions. Privacy protection approaches aim at hiding user's identity and/or some part of the personal identifiable information (PII), whereas privacy management offers transparency to the DS concerning the collection and processing of PII.

Trust can be understood as the subjectively perceived probability by a DS that a system will perform an action before the DS can monitor it [4]. It indicates uncertainty about the features of communication partners [5,6]. Trust is also context-dependent and the ways it is formulated vary, for example, it can be based on the recommendation received from others, it can be reputation-based, or it may be a subjective degree of belief of others [7,8].

Privacy and trust are interrelated concepts, that is, "data disclosure means loss of privacy, but an increased level of trustworthiness reduces the need for privacy" [1]. The DS interest is to get maximum benefit from services and at the same time to minimize the loss of privacy.

In health care, internationally accepted principles, good practice rules, and domain-specific legislation define patient's rights and service providers' responsibilities. Health care-specific legislation also states how patient's privacy must be protected [1]. Researchers have started to develop such kind of principles for ubiquitous health. Ruotsalainen et al have developed the THEWS (Trusted eHealth and eWelfare Space) principles for trustworthy ubiquitous health. The THEWS principles state that the DS possesses the right [1]: to verify the trustworthiness any system that collects or processes his or her personal health information (PHI). Principles state that DS should also have the right for controlling the processing of PHI, both inside the systems and between them. DS should define personal privacy policies, which regulate how his or her health data is collected, processed, disclosed, shared, stored, or destroyed. The principles also require the DS to be aware of all events, situations, and contexts where his or her health data is collected, processed, stored, and disclosed.

Furthermore, systems and stakeholders have the responsibility to publish information needed for trust verification and support openness and transparency of data processing.

Ubiquitous health features and its ubiquitous environment suggest that trustworthiness and privacy are real concerns [9,10]. In ubiquitous health, it is difficult to understand the processing of data inside the systems [11], as systems do not always perform in accordance with their policies, and the privacy preferences of DS might conflict with the business objectives of the system [12]. As a result, the DS cannot assume that the existing legal framework guarantees the processing of PHI lawfully and according to the rules proposed by him or her [13,14]. In addition, DS also cannot assume that systems have implemented security rules and functional privacy requirements derived from laws and standards [1,15]. A big challenge in ubiquitous health is that different stakeholders (eg, systems, customers, third parties, and regulators) can have their own privacy policies.

Here we hypothesize that in order to be successful, ubiquitous health requires trustworthiness and privacy management made by the DS. Without these two features, DS will not dare to use its services. Furthermore, the architecture supporting ubiquitous health should fulfill the THEWS principles presented above. As traditional security and trust mechanisms used in today's health care information systems may not provide adequate security and privacy in ubiquitous health [1,2,16], a novel architecture is required.

Prior Work

The development of ubiquitous systems and the growing use of ubiquitous computing have raised the following question: What kind of trust and privacy models, services, and architectures offers acceptable level of privacy and trustworthiness?

Trust Models

Trust models such as belief, organizational trust, dispositional trust, recommended trust, and direct trust have been proposed for pervasive systems [8,17,18]. Dispositional trust describes the general trusting attitude of the trustor [17]. Direct trust is derived from the outcomes of interactions with peers [19]. In recommended trust, an agent makes a recommendation based on the beliefs that other entity is trustworthy at certain degree. Organizational or institution-based trust is based on the

perceived properties of, or the reliance placed on, a system or institution [7]. Reputation is a recommended rating based on the opinions of others [8]. All of them are situational, that is, the amount of trust that a DS experiences depends dynamically on situation and service-specific trust features [20,21].

A trust is typically based on the trustor's characteristics such as ability, integrity, and benevolence and should not be a blind guess [5]. It is expressed either by value, rating, or ranking or as probability or belief [22]. Trust attributes such as integrity, motivation, competence, and predictability are proposed to measure the confidence level [23]. Attributes proposed by Hussin include trustee's identifier, certificate, ability, predictability, trustee's privacy policy, legal requirements, and system's properties such as transparency, authenticity, confidentiality, and nonrepudiation [24]. Researchers have developed mathematical methods such as Bayesian probability, Beta probability, maximum likelihood, game theory, weighted arithmetic means, and average of weighted recommendations to measure the degree of belief or recommended trust [25-27]. Trust degree can also be measured from interaction frequencies between trustor and trustee [28], or from context-dependent direct and indirect recommendations collected from selected users [19].

In contrast to belief and recommended trust, computational trust built on abstractions of human concept of trust has been proposed by researchers [25,29]. Within ubiquitous computing, computational trust means automation of decisions in the presence of unknown, uncontrollable, and possibly harmful agents [29]. Computational trust value has been calculated using trustor's experience, recommendations, interactions, knowledge, measurements, distance, and density of events [13,25,28,30,31]. Service level agreements, contractual agreements, reputation based on the brand's name, trust manifesto, trust negotiation, exchanging and evaluating credentials, and recommendations made by a trust authority (TA) are also widely used in commercial eServices [32,33].

The aforementioned trust models have noticeable weaknesses in ubiquitous environment. Recommendations are unreliable because they are based on unsecure opinions. It is difficult to force everyone to accept certificates or common TA, and many virtual organizations do not have connection to it. A common ontology that is required for successful negotiation and calculation of trust attributes seldom exists. Trust manifesto assumes that the DS blindly trusts that service providers will deliver their promises. Furthermore, the reliability of reputations is difficult to measure, and credentials are difficult to evaluate [25].

Privacy Models and Formula

Many privacy models developed by researchers are useful in ubiquitous environment. Lederer et al proposed a model of situational faces [34]. The model proposed by Hong et al uses control and feedback [10]. The model suggested by Friedwald et al included actors, environment, activity, information flow, control level, and enabling technology [35]. Adams and Sasse look at privacy as preferences and constraints, and use a computer-understandable language for expressing them [36]. Jiang and Landay used an information space model [37], and Kapadia et al applied virtual walls for privacy management [38]. Diaz et al proposed entropy as measure of privacy level [39].

Privacy management model proposed by Lederer et al combined Adams's perceptual model and Lessing's societal privacy models [40,41]. In the model by Lederer et al, a preferred privacy level depends on legislation, market features, norms, technology used, nature of personal information disclosed, contextual features, information sensitivity, characteristics of information user, and expected cost-benefit ratio. A limitation of this model is that its variables are qualitative and abstract.

Trust and Privacy Technologies and Solutions

Numerous trust and privacy technologies have been proposed for ubiquitous systems. In Gray's solution, the trust is based on the belief of a person that systems have implemented proper de-identification structures and safeguards. It also includes a compliance checker and a trust value calculator [42]. PoliCyMaker, KeyNote, Simple Public Key Infrastructure, and Pretty Good Privacy solutions use credentials [43]. The Trust-X approach by Bertino et al uses digital credentials, which are iteratively disclosed and verified [32]. Becerra et al proposed intelligent agents to evaluate which other agents can be trusted [23]. According to the Skopik's approach, rule-based trust interpretation takes into account the subjective nature of trust [44]. Joshi et al noted that it is possible to make security and privacy decisions based on trust attributes [45].

Computational trust is either based on direct measurements, observed (monitored) features, or past experiences [46]. In ubiquitous environment, successful monitoring requires common ontology and measurable indicators [22]. The trust manager architecture proposed by Salah et al collects trust aspects for calculator that computes a trust score. The architecture also includes recommendation manager, monitor services, context provider, log service, and policy manager [47]. In the EnCoRe architecture, the TA keeps track of promises, manages decryption keys, discloses them, and verifies systems properties [48]. Thereby, the customer should trust on the system's released willingness to fulfill the personal policies of DS.

Privacy is often protected by using privacy enhancement solutions such as data filtering and minimization, anonymization, and adding noise to disclosed information (eg, data hashing, cloaking, blurring, and identity hiding) [41,49]. In metadata approaches, privacy policies can be injected to application, tagged to the metadata, or added to the database or an active agent [50]. Berghe and Schunter's "privacy injector" adds privacy rules to existing applications [11]. The EnCoRe architecture uses the sticky policy paradigm where the DS can stick machine-readable rules to the data before it is disclosed [48]. Metadata can include embedded (active) code that enables self-destruction (apoptosis) in the case the environment is not trusted [51]. Apoptosis can also be context- or situation-aware (ie, programmed death) [52]. As per Pallapa et al, active privacy metadata dynamically controls the transparency of data in a context [53].

Other solutions also exist for privacy protection. Kapadia et al created a virtual personal space (a room) to control information

flow through its "walls" [38]. In the PICOS platform from Kahl et al, a privacy advisor helps the DS to create own policies [54]. In the United States, a flexible approach that uses privacy and security labels is under development. In this standardized solution, PHI is segmented and security and privacy labels are bound to those segments [55].

In pervasive systems, privacy requirements are typically expressed as policies that are context-dependent. Policies define what is permitted or prohibited, and which are permitted actions [45]. From the DS viewpoint, policy can be understood as a statement (rules) about how a certain system should behave [56]. Policies are typically published in the form of credentials or metadata, and rules are expressed using policy language [33]. The successful use of policies requires policy matching, mismatch notification, policy lifecycle management, risk analysis, regulatory compliance checking, and possibility to model privacy regulations [48,57]. It is also necessary that the DS can enforce personal polices [58]. Policies should also be checked for ontological compatibility [59].

The increasing use of the Internet, peer-to-peer systems, multi-agent systems, and social networks has been main drivers for discussed privacy and trust models and solutions. Unfortunately, most of them are focused on one feature (eg, encryption or context). Ubiquitous health requires much wider approach. Like Bryce et al, we also state that pervasive systems require an architecture that combines dynamic privacy policies, a priori trust validation, privacy management, and a posteriori measurement (ie, feedback) what systems are doing [2]. Regulatory compliance is also needed.

In this paper, we propose a novel privacy management architecture for ubiquitous health. As ubiquitous health is a new concept without widely accepted principles and privacy and trust models, it is necessary to select on which principles and models the architecture is based. THEWS principles, as previously presented, have been selected by the authors on the basis of the architecture, that is, the architecture should be compliant with them. The solution should take into account features of ubiquitous health and enable the DS to dynamically manage the privacy by defining system-specific privacy policies. The architecture should mimic the way humans use trust information in creation of personal policies. The architecture should also offer protection against many known privacy threats existing in ubiquitous environment.

Methods

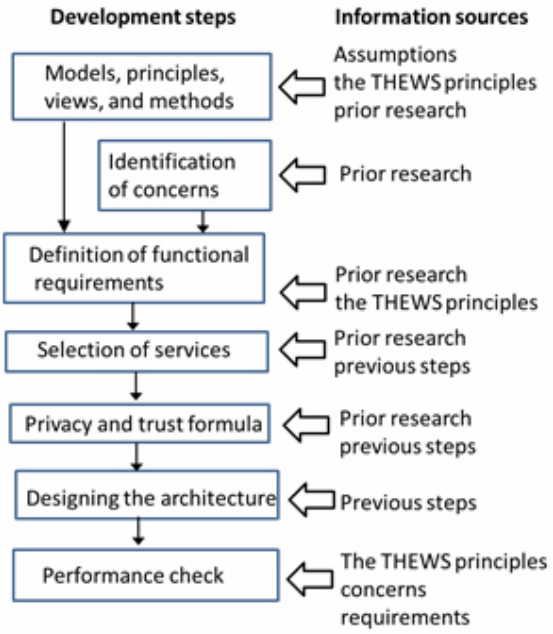
From system theory and systems engineering perspectives, ubiquitous health is a metasystem that is characterized by its structure, its function/behavior, and how its interrelated components are composed in an ordered way. Instead of creating artificial scenarios or making quantitative privacy risk/threat analysis, a more system-oriented sequential method that combines methodologies used in systems engineering, requirement analysis, and system design is used (Figure 1).

The method used in this study includes the following steps: definition of basic requirements; selection of values, privacy and trust models, and views; identification of concerns; definition of functional requirements; selection of services; developing privacy and trust formula; and designing the architecture. Finally, it is checked how the architecture meets purposes and requirements for which it has been intended.

On the background of processing of health information stay ethical values and codes, principles, and common rules. Selection of these features has also strong impact on the architecture and its services. For some environments (eg, health care), widely accepted codes and rules already exist; however, this is not the case in ubiquitous health. Therefore, the first step is to select privacy and trust models and approaches that are in line with principles and without noticeable weaknesses. This is achieved by carefully analyzing existing research published in journals, conference proceedings, and standards documents. Similarly, identification of concerns and definition of functional requirements are also done. Finally, the architecture combines selected services in such a way that principles and requirements are fulfilled.

In this paper, privacy and trust needs are examined from the DS's viewpoint. Other views are not discussed. To reduce the complexity, only components that are relevant for the privacy management needs of the DS are included in the architecture.

Figure 1. Method for the development of the THEWS architecture.



Results

General Overview

Ruotsalainen et al have noted that privacy rules in ubiquitous health are based on trust [1]. Therefore, privacy and trust models selected should take into consideration features of ubiquitous health, trust and privacy aspects of systems offering health services, regulatory requirements, and the DS's privacy needs. The asymmetric relationship between systems providing health services and the DS should also be considered (ie, the DS seldom has the power to force a system to put personal rules into effect). Furthermore, in practice, the DS has no tools to make personal observations of systems' internal security and privacy features and policies [51,60].

Principles, Models, and Views

In spite that privacy is widely accepted as human right (value), different privacy models do exist in real life. Regulatory and self-regulatory models are widely used [15]. Privacy can also be considered as personal property [20]. Regulatory model is insufficient in ubiquitous environments [13], and self-regulation made by business community gives systems as stronger partner much freedom to set rules [15]. Because in ubiquitous health the DS has the right to set personal rules to regulate and control his or her health information, self-regulation model that uses privacy as the DS's personal property has been selected for the architecture.

Suitability of widely used privacy protection and management approaches in the context of ubiquitous health is shown in Table 1. Based on Table 1 and the fact that pervasive systems require dynamic and context-aware privacy management [46], the foremost privacy approach for ubiquitous health is privacy management that uses context- and content-aware policies and supports transparency and regulatory compliance.

Trustworthy ubiquitous health requires that used trust model enables the DS to work out the level of trustworthiness of systems. Characteristics and weaknesses of widely used trust models in regard to features of ubiquitous health are shown in Table 2. As a result, trust in ubiquitous health cannot be based on the belief or reputation, and the DS usually does not have a right to verify recommended trust. Credentials typically assume that Hobson choice and privacy labels have inappropriate granularity. Although some researchers assume that the protection power of laws is sufficient and certification offers acceptable level of trust [12], the regulations and certificates are found to be insufficient in ubiquitous health.

Computational trust that is based on systems' measurable or observed properties can offer reasonable information to the DS in designing personal privacy policies [25]. The limitation that the information content of a single trust value is too low for policy formulation [61] can be overcome by using additional system-specific attributes. Therefore, computational organizational trust with attributes is selected as the trust model for ubiquitous health.

From the DS viewpoint, the architecture should mimic humans' ways to design policies, support more rational choices than intuition, and give feedback to the DS. Louviere's stated customer choice method fulfills these requirements by including awareness, learning, evaluation and comparison, preference formulation, and choice and post-choice [62]; hence, it is selected for the method that the DS uses in the formulation of privacy policies.

Table 1. Suitability of common privacy protection and management approaches for ubiquitous health.

Approach	Suitability
Privacy protection using security services (eg, authentication, authorization, and access control)	Security cannot offer reasonable level of privacy in ubiquitous health. Access control alone is insufficient. The DS is not familiar and cannot control authorization rules used inside a system
Privacy control by hiding the DS's identity	Health care and health services require the knowledge of the DS's identity
Delegation approach	Delegation requires knowledge to whom the DS delegates access rights. Systems specifically do not publish this kind of information to the DS
Privacy labels	Rules deployed in a label might be inadequate and in conflict with the DS policy that may or could not be specified in labels
Privacy management using context- and content-aware policies	Supports dynamic policies, but requires computer-understandable policy language. Common ontology, ontology harmonization (matching, mapping, etc.), or reasoning is needed
Metadata approach	All systems do not accept injected or active code
Data filtering and adding noise to data	Health services require large amount of PHI for correct and effective services, as incomplete PHI can lead to wrong decisions or prevent the use of services

Table 2. Characteristics and weaknesses of common trust models.

Model	Characteristics and weaknesses in ubiquitous health
Dispositional trust and recommended trust	Characteristics: Based on belief, attitude, or others' opinions (recommendations)
	Weakness: Recommendations are unreliable and based on unsecure opinions. It is difficult or even impossible to check the reliability of others' recommendations
Blind trust	Characteristics: Based on belief or attitude that organization has implemented sufficient safeguards
	Weakness: Does not guarantee trustworthiness
Predefined trust	Characteristics: Based on assumption that an organization has implemented required regulatory services
	Weakness: Static model. Unsuitable for dynamic environments.
Trust label	Characteristics: Based on organizational or personal labels
	Weakness: Inappropriate granularity and insufficient consideration of dynamic contextual conditions
Trust manifesto	Characteristics: Based on assurance of service provider
	Weakness: Based on belief or attitude. The DS should blindly trust
Reputation	Characteristics: Based on subjective opinions of others
	Weakness: The reliability of reputations is difficult to measure
Computational trust	Characteristics: Based on system's measured or observed features
	Weakness: A simple trust value or rank might offer insufficient information for the DS in designing personal policies
Risk- and threat-based models	Characteristics: Based on risk or threat assessment
	Weakness: Difficult or even impossible to measure personal privacy risks
Trust management using credentials	Characteristics: Based on credentials issued by authorities. It is targeted to create trust between organizations
	Weakness: Credentials are static. Difficult to evaluate and require a network of trusted authorities. It is difficult to force everyone and virtual systems to accept credentials or a TA

Identification of Concerns

Typical stakeholders in ubiquitous health are the DS, health service providers, other organizations, and secondary users. Different stakeholders have different concerns [1]. This paper is focused to the DS concerns. The main concerns of the DS are as follows: (1) how trustworthy the system is, (2) why is lack of awareness and transparency in data collection and processing, (3) who is using the data inside a system, (4) how to guarantee that data is processed lawfully, and (5) according to the DS's policies, how to prevent post-release of data and control unnecessary secondary use.

Functional Requirements

Derived from previously mentioned assumptions and selections and the proposals made by other researchers, the architecture

should identify the following functional requirements. The architecture should offer tools for the DS to define purposes of data collection, express computer-understandable rules regarding the sensitivity of data elements, design protection needed, rule how long data is stored, and which data is disclosed and for what purposes [14,48].

The architecture should support dynamic content-, context-, and purpose-aware privacy management. It should also offer to the DS system-specific computational trust information with attributes that describe systems' features, infrastructures, policies, and relations in advance. Humans' way to design policies, to support more rational choices than intuition, and to give feedback should need to be mimicked. The architecture must be compliance with Louviere's stated customer choice method. It should support situations where the DS discloses PHI and where data collection or disclosure is made autonomously by a system. The architecture also enables the DS to be aware of data-processing events, and to set policies regulate the secondary use and reuse of PHI.

Trust and Privacy Services

Services of the architecture should fulfill above-mentioned requirements, and take into account expected concerns. Trust and privacy services selected for the THEWS architecture are shown in Table 3.

Table 3. Trusts and privacy services for the THEWS architecture.

Concern/Function	Service
System's trustworthiness	Trust calculation service
	Context service
	Identification service
	Trust interpreter service
The DS's information autonomy	Decision support service
	Policy-binding service
Awareness and transparency	Monitoring, trust calculation, and notification services
The use of PHI inside the system	Monitoring and notification services
Does the system use PHI according to the DS's policies	Monitoring and notification services
Choice and secondary use and post-release of PHI	Policy-binding service
	Metadata (eg, sticky policy or active code for apoptosis)
Designing privacy policies and comparison and preference formulation	Decision support service
Policy formulation and post-choice and new policy creation	Policy management service
	Policy assistant service
	Ontology service
System's features and relations	Trust calculation service
Feedback and alarm or conflict notice	Monitoring service
Learning	Trust interpreter and policy assistance services

Privacy and Trust Formula

The THEWS principles and functional requirements determine that the DS can use trust information in the formulation of privacy policies [1]. The following formula has been developed to illustrate how trust information, privacy variables, and privacy policy are related:

Privacy_policy=f(TI, IS, SE, PU)

In this formula, TI refers to *trust_information* offered by the architecture to the DS. IS, SE, and PU are privacy variables proposed by Lederer [40]. IS refers to the sensitivity of the data, SE describes the situation where information is used, and PU defines the purpose of data collection or use.

To avoid the drawback of a single calculated trust value and to enable attribute-based creation of personal policies [61], the following trust information formula was developed:

Trust_information=Trust_value+Trust_feature_vector

Trust_feature_vector gives the system- and environment-specific information to the DS about systems' regulatory compliance and their willingness to follow the DS's policies and support openness. Slightly modified trust attributes originally proposed by Hussin et al have been selected for trust value calculation [24]:

Trust_value=(E, T, P, PO, Pre, Tran, Ab)

where E represents domain specific environmental factors such as legal requirements and system's contextual features. T represents the type of service provider's organization (eg, public health care provider, private health service provider, Internet service provider). P (properties) consists of systems architectural and technological aspects and PO is system's privacy policy. Predictability (Pre), transparency (Tran), and ability (Ab) are different parameters that can be calculated from the system's

past history or by direct measurements. For *Trust_feature_vector*, the following formula was developed:

Trust_feature_vector=(DGD, DRB, SPO, DSP, ASP, CD, ATV, AUT, RP, PBL, DSA)

where DGD and DRB describe the level of system's regulatory compliance. The DGD is the degree of data processing made by the system in compliance with international privacy protection directives. The DRB is the degree of data processing performed by the system compliant with health care-specific laws and rules. SPO and RP are parameters that are related to openness. SPO informs if the system has made its privacy policies openly available, and RP tells the status if the system has published its relationships. DSP, ASP, ATV, and AUT are willingness parameters. DSP describes the degree by which the system follows its own privacy policies. ASP informs that the system either enables or rejects the DS to inject personal policies to PHI collected or processed by the system. The ATV expresses whether the system accepts external monitoring of events related to the processing of PHI, and AUT tells whether the system enables external access to its audit trails. The PBL and CD are trustworthiness parameters. CD informs whether the system has been certified, and PBL informs about the position of the system on the blacklist. The DSA is an optional attribute that can be defined by the DS. For DGD and DRB, a linear scale (0...1) is used, whereas all others attributes have only binary values. In case of no or insufficient data, the attribute value is zero.

Using proposed *Trust_information*, the DS can predict system's willingness or ability to process PHI legally and follow rules set by the DS. The *Trust_information* informs the DS about how much it can trust on a system, how system's policy and technical architecture look like, and to what extent system's policy is compliant with domain-specific regulations and laws. If needed, the DS can use attributes to mark a system untrusted (eg, in the case it will not publish its policies nor would accept monitoring). Most attributes can be calculated from information the system has, or should have, published; however, some attributes might require direct observations. Attributes such as DSP can be calculated from the system's past history.

The THEWS Architecture

A layered framework model that describes trust and privacy services of the THEWS architecture is shown in Figure 2. The top layer of the model consists of common services that are offered to all stakeholders. The middle layer includes privacy and trust services needed. Ubiquitous health, stakeholders, other users, and PHI are located in the lowest layer (ie, network layer).

As it is difficult or even impossible for the DS to evaluate the trustworthiness of systems, an independent agent, the trust calculator (TC), is used for this task. The role of TC is not to make trust decisions. Similar to HL7 Privacy, Access and Security Services architecture, the TC should be understood as an information point that sends trust information to the DS [55].

The TC calculates *Trust_information* (ie, *Trust_value* and related *Trust_feature_vector*) by using the information that system has published, and available contextual data, system's measured or monitored features, and system's past history. It also detects malicious or fake systems by using information obtained from context and monitoring services. Two assistance services are offered to the DS: (1) trust interpreter and (2) policy assistance service. The DS can use the trust interpretation to understand the meaning of received *Trust_information*.

The context service collects systems' contextual data, interprets it, and makes it available to TC and DS, using ontologies. The DS deploys policy management, policy-binding, policy assistance, and decision support services in policy formulation.

The monitoring service offers feedback, reduces risk, and recognizes policy conflicts. It records and assesses how a system in real life processes PHI. It recognizes policy conflicts and alarms the TC and the DS of possible malicious or illegal use of PHI. The notification service works as communication and transparency tool between the DS, systems and services. Using this service, the DS expresses personal policies to systems that in turn publish their policies and relations.

An architectural model describing the interconnection of the THEWS services is shown in Figure 3. In the architecture, the policy formulation is a decision-making process, where the DS chooses privacy rules, privacy management services, and the amount of PHI he or she wants to trade in according to expected service benefits. The selected rules and services depend on privacy needs, *Trust_information*, and the purpose of data request. Typical privacy management services that can be activated before data disclosure are encryption, anonymization, and data filtering. The DS may also inject policies and/or active code to the metadata.

The THEWS architecture not only fulfils the THEWS requirements but also offers protection against many of the known privacy threats existing in pervasive systems as shown in Table 4.

Figure 2. The framework model for the THEWS architecture.

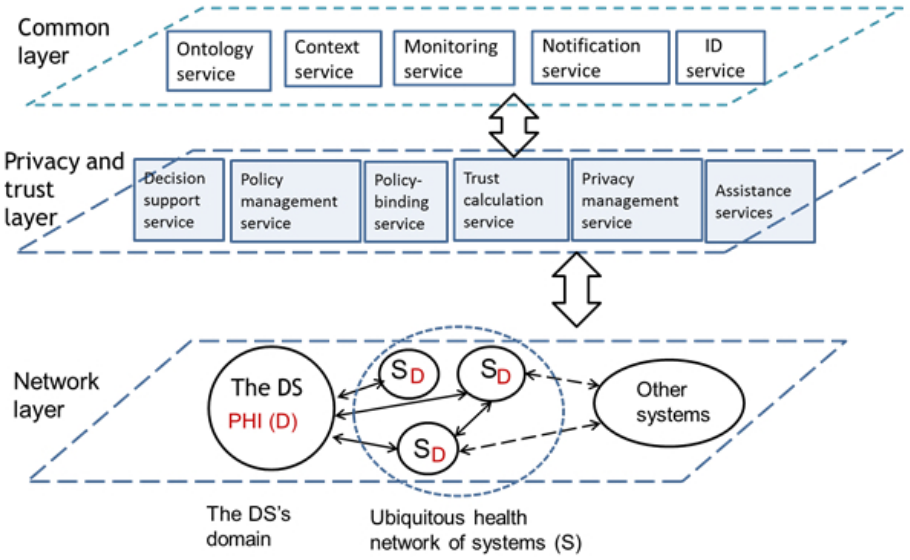


Figure 3. The interconnection of privacy and trust services in the THEWS architecture.

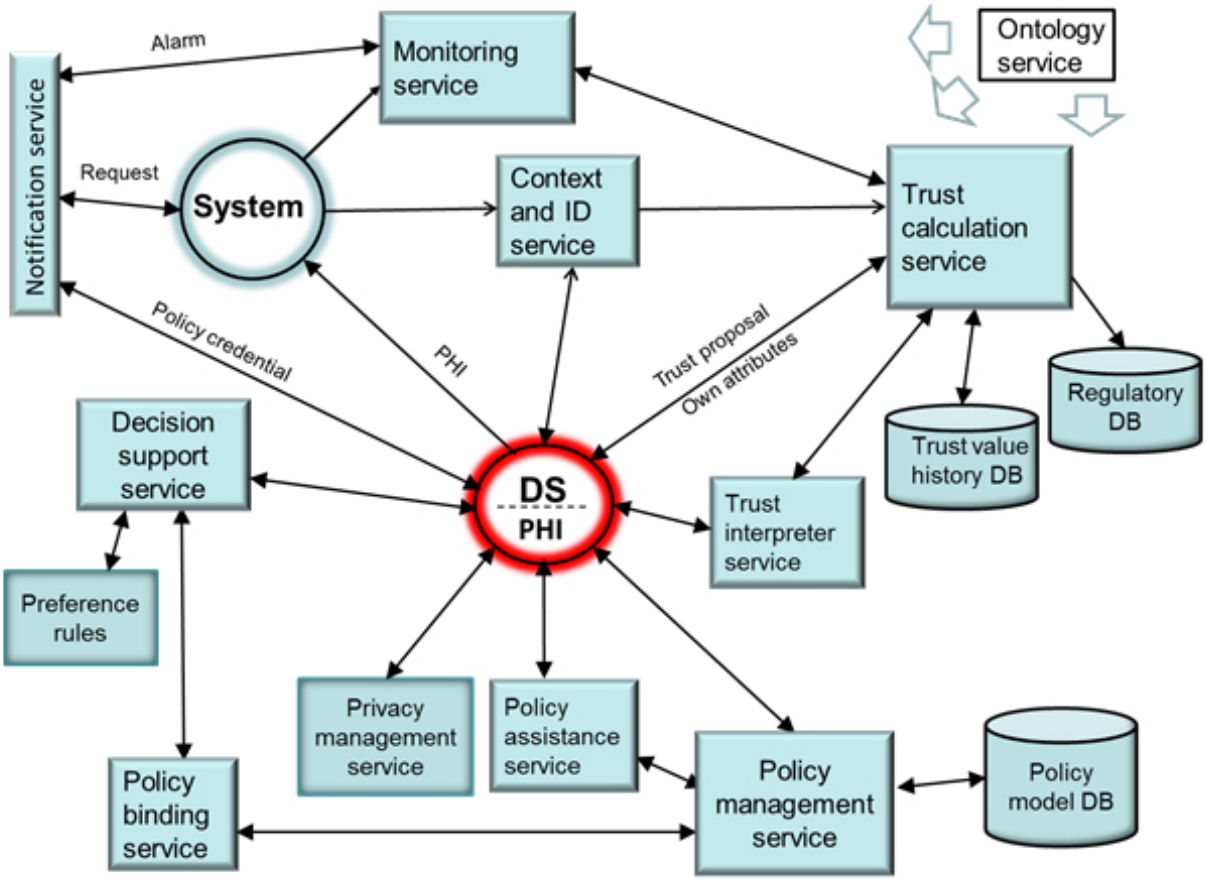


Table 4. The THEWS architecture approach for the challenges existing in pervasive systems.

Challenges and threats	THEWS approach
Pervasive systems are dynamic in nature (eg, ad hoc networks) where static rules and privacy services will not work	Dynamic rules and services are used
	Dynamic creation and management of the DS's privacy service portfolio
No predefined trust	Dynamic trust calculation based on systems' measured properties
The need of PII is dynamic and purposes are unpredictable	Dynamic context-aware polices support ad hoc purposes
Organizations do not always follow their own policies, and laws will be ineffective without sufficient control and penalties	The way systems process PHI is dynamically monitored, and the regulatory compliance is checked
Users want to control how systems use PII	The DS define system-specific policies that rule the use, storing, and sharing of PHI
It is difficult to know what is the actual privacy status of an enterprise (ie, what data and under what policy)	Status and policies are inspected and informed dynamically to the DS
It is difficult to know how data has been used inside the enterprise	The monitoring service can check internal use
Relationships between systems can be unknown	Systems must publish their relations
All service providers do not use certificates	Trustworthiness is not based on certificates
Selection of service provider needs trust and/or reputation	The TC offers calculated trust value and trust attributes to the DS
	Reputation is not used
Determining of systems' trustworthiness is challenging	The TC calculates trust using direct measurements
	The monitoring service gives feedback to the TC
Which action the DS must take in the case of privacy breach?	The TC and/or monitoring service inform the DS of privacy breaches
	The DS can change policy dynamically
How to guarantee that data is processed lawfully and according to the DS's policies	Trust attributes offer required information
	The monitoring service notifies misuse
Lack of awareness	Systems must publish their rules and relationships
	Awareness by monitoring service
How to know what actions are permitted or forbidden in a context and what actions must be performed?	The DS defines personal context-aware rules
How we can trust on systems privacy notices (or privacy manifesto)?	Privacy notice/manifesto is not used
Threats caused by surveillance, identity theft, or malicious attacks	Communication platform and systems must implement reasonable safeguards
Code of conduct, legal framework, and accreditation of centers will not guarantee trustworthiness	Those models are not used
Consent does not guarantee adequate protection	Consent is only one possible item in the policy
Anonymization such as "we know" will not guarantee adequate protection	Anonymization is only a value-added service
Secondary use of PII must be monitored	Monitoring service
Citizens need audit information	The monitoring service assesses the audit log and informs findings to the DS
	The TC can maintain a list of untrusted or malicious systems
Data requestors can have subjective views of trust	The TC defines the used trust ontology
How can we manage trust for systems with incomplete credentials?	Credentials are not used

Discussion

In this study, novel privacy architecture is developed for ubiquitous health. It enables the DS to ensure and manage information privacy by choosing personal context-aware privacy policies for each system with the help of computational trust information that includes a trust value and system-specific trust attributes. The architecture combines many trust and privacy services proposed by researchers for pervasive systems such as trust calculation and interpretation, policy management, policy assistance, policy binding and design, and context services and

monitoring. The architecture goes far beyond the security services with traditional access control used in health care, and it also illustrates how the THEWS principles can be realized. Furthermore, the architecture offers protections against many privacy threats caused by ubiquitous computing and unsecure environment. Instead of continuous validation of systems' trustworthiness, the architecture monitors functioning of the systems, detects and informs the DS of policy conflicts and data misuse, and thereby enables the DS to dynamically change policies.

Contrary to a widely used trust manifesto that is based on incomplete, insufficient, or inconclusive information [33] or a single trust value that offers only Hobson's choice to the DS, the architecture gives information to the DS that indicates the level of transparency and openness of a system, how system follows health-specific privacy rules and regulations, and how mature the system is to accept the DS's policies. Using this information and policy assistance, decision support, and policy-binding services of the architecture, the DS can construct context- and content-dependent policy profiles and assign them to systems. The architecture is user-friendly, and there is no need to interactively calculate the trust value against the DS's dynamic privacy needs.

For all pervasive systems, some of the unsolved privacy challenges are as follows: (1) How to prevent data from being collected and used in a way that DS cannot recognize? (2) How to prevent systems for breaching their promises? and (3) How to prevent the misuse of PHI after it has been released for secondary use?

Regulation and monitoring can give partial solution to first two challenges. Policy agents, self-destroying files, programmed death (apoptosis), destruction of cryptographic keys, and mutation engines have been proposed by researchers to give protection in the case of post-release [52,63]. The flexibility of developed architecture enables the DS to deploy any of these engines to control the secondary use of PHI.

In addition, there remain some more important challenges. The TC should understand both international and national regulations, and rules used by systems. Translation of narrative rules into machine-readable policies is an ongoing challenge [14]. The use of computer-understandable and context-aware polices requires either that all stakeholders accept a common policy language (such as Ponder, KAoS, Security Assertion Markup Language, eXtensible Access Control Markup Language, Rei, XPath-Based Preference Language, P3P, and APPEL) or that they use a method that enables semantically correct transformation between languages, based on ontologies [43,64,65]. Meta-policies such as P3P and Rei are candidates for the latter case [64,66,67]. In ubiquitous health, the use of a single policy language and a common ontology might be impossible. A possible solution is that the TC and the DS simply inform to systems about the ontology and policy language they use. If this is not possible, a service that maintains interoperability between policy languages and offers ontology reasoning should be developed [68]. In addition to policy, context and trust ontologies and other ontologies such as information and communication technology ontologies that describe systems' architectural and organizational aspects and mechanisms are needed. Considering the future work, the authors will evaluate the architecture, and validate its feasibility and functionality in pilot setting. As a minimum, the proof of concept will be done. The authors will also demonstrate that the proposed solution is technically valid, safe to use, and efficient.

Acknowledgments

The results presented in this paper are based on the findings of the Trusted eHealth and eWelfare Space (THEWS) project. The project was supported by the Finnish Academy during 2009-2012 via the MOTIVE research program.

Conflicts of Interest

None declared.

References

1. Ruotsalainen PS, Blobel BG, Seppälä AV, Sorvari HO, Nykänen PA. A conceptual framework and principles for trusted pervasive health. J Med Internet Res 2012 Apr;14(2):e52 [FREE Full text] [doi: 10.2196/jmir.1972] [Medline: 22481297]
2. Bryce C, Dekker M, Etalle S, Le Metayer D, Minuer S. Ubiquitous privacy protection. 2007 Presented at: First IEEE International Workshop on Privacy in Ubiquitous Systems; August 2007; Salzburg, Austria URL: http://hal.inria.fr/inria-0039510 [WebCite Cache]
3. Westin AF. Social and political dimensions of privacy. J Social Issues 2003 Jun;59(2):431-453. [doi: 10.1111/1540-4560.00072]
4. Gambetta D. Trust: Making and Breaking Cooperative Relations. New York, NY, USA: B Blackwell; 1988. Can we trust URL: http://www.loa.istc.cnr.it/mostro/files/gambetta-conclusion_on_trust.pdf [WebCite Cache ID 6JmR4xmeS]
5. Schoorman FD, Mayer RC, Davis JH. An interactive model of organizational trust: past, present and future. Acad Manage Rev 2007 Apr 01;32(2):344-354. [doi: 10.5465/AMR.2007.24348410]
6. Ruohomaa S, Kutvonen L. Trust management survey. In: Herrmann P, Issarny V, Shiu S, editors. Trust Management: Third International Conference, iTrust 2005, Paris, France, May 23-26, 2005, Proceedings. Heidelberg: Springer-Verlag; 2005:77-92.

7. Abdul-Rahman A, Hailes S. Supporting trust in virtual communities. 2000 Presented at: Proceedings of the 33rd Hawaii International Conference on System Sciences; Jan 4-7, 2000; IEEE Computer Society, Washington, DC, USA. [doi: 10.1109/HICSS.2000.926814]
8. Billhardt H, Hermoso R, Ossowski A, Conteno R. Trust-based service provider selection in open environments. New York, NY, USA: ACM; 2007 Presented at: Proceeding of the ACM Symposium on Applied Computing; 2007; Seoul, Korea p. 1375-1380. [doi: 10.1145/1244002.1244298]
9. Bellotti V, Sellen A. Design for privacy in ubiquitous computing environment. In: ECSCW '93: Proceedings of the Third European Conference on Computer-Supported Cooperative Work, 13-17 September 1993, Milano, Italy. Dordrecht: Kluwer Academic Publishers; 1993:77-92.
10. Hong J, Ng DJ, Lederer S, Landay JA. Privacy risk models for designing privacy sensitive ubiquitous computing systems. : ACM; 2004 Presented at: Human-Computer Interaction Institute; Aug 1-4, 2004; Cambridge, MA, USA URL: http://repository.cmu.edu/hcii/69 [WebCite Cache]
11. Berghe CV, Schunter M. Privacy injector – automated privacy enforcement. Berlin, Germany: Springer; 2006 Presented at: Proceedings of the 6th International Conference on PET; 2006; Cambridge, UK p. 99-117. [doi: 10.1007/11957454_6]
12. Skinner G, Han S, Chang E. A new conceptual framework within information privacy: meta privacy. In: Hao Y, Jiming L, Wang Y, Cheung Ym, Yin H, Jiao L, et al, editors. Computational Intelligence and Security: International Conference, CIS 2005, Xi'an, China, December 15-19, 2005, Proceedings, Part II (Lecture Notes in ... Notes in Artificial Intelligence) (Pt. 2). Berlin: Springer; 2005:55-61.
13. Yan Z, Holtmanns S. Trust modeling and management: from social trust to digital trust. In: Subramanian R, editor. Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions. London, UK: IRM Press; 2007.
14. Mont MC, Pearson S, Creese S, Goldsmith M, Papanikolaou N. Towards a Conceptual Model for Privacy Policies - HPL-2010-82. USA: Hewlett Packard; 2010. URL: http://www.hpl.hp.com/techreports/2010/HPL-2010-82.html [WebCite Cache ID 6GtlD94r5]
15. Zwick D. Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce.: University of Rhode Island; 1999 Sep 07. URL: http://ritim.cba.uri.edu/Working%20Papers/Privacy-Models-Paper%5B1%5D.pdf [accessed 2013-05-26] [WebCite Cache ID 6GtkWin5q]
16. Campbell R, Al-Muhtadi J, Naldurg P, Sampemane GM, Mickunas MD. Towards security and privacy for pervasive computing. In: Okada M, Pierce BC, Andre S, Hideyuki T, Yonezawa A, editors. Software Security - Theories and Systems : Mext-NSF-JSPS International Symposium, ISSS 2002, Tokyo, Japan, November 8-10, 2002. Berlin, Germany: Springer-Verlag; 2002:1-15.
17. Abdul-Rahman A, Hailes S. A distributed trust model. 1997 Presented at: Proceedings of the 1997 Workshop on New Security Paradigms; 1997; ACM, New York, NY, USA p. 48-60. [doi: 10.1145/283699.283739]
18. McKnight DH, Choudhury V, Kacmar C. Developing and validating trust measures for e-commerce: an integrative typology. Inform Sys Res 2002 Sep;13(3):334-359. [doi: 10.1287/isre.13.3.334.81]
19. Uddin GM, Zulkernine M, Ahmed SI. Cat: a context-aware trust model for open and dynamic systems. New York, USA; 2008 Mar Presented at: Proceedings of the 2008 ACM Symposium on Applied Computing; Mar 16-20, 2008; Brazil p. 2024-2029. [doi: 10.1145/1363686.1364176]
20. Sabater J, Sierra C. Review on computational trust and reputation models. Artif Intell Rev 2005 Sep;24(1):33-60. [doi: 10.1007/s10462-004-0041-5]
21. Liu Z, Yau SS, Peng D, Yin Y. A flexible trust model for distributed service infrastrucure. USA: IEEE; 2008 Presented at: Proceeding of the 11th Symposium on Object Oriented Real-Time Distributed Computing (ISORC); May 7-5, 2008; Orlando, USA p. 108-115. [doi: 10.1109/ISORC.2008.84]
22. Ries S. Trust in Ubiquitous Computing (PhD thesis). Darmstadt: Technischen Universitet Darmstadt; 2009. URL: http://tuprints.ulb.tu-darmstadt.de/id/eprint/1948 [WebCite Cache ID 6JfIn6NxS]
23. Becerra G, Heard J, Kremer R, Denzinger J. Trust attributes, methods, and uses. 2007 Presented at: Proceedings of the Workshop on Trust in Agent Societies, AAMAS-2007; May 15, 2007; Honolulu, Hawaii, USA p. 1-6 URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.6965&rep=rep1&type=pdf [WebCite Cache]
24. Hussin Ab RC, Macaulay L, Keeling K. The importance ranking of trust attributes in e-commerce Website. 2007 Presented at: Proceedings of the 11th Pacific-Asia Conference on Information Systems; Jul 3-7, 2007; Auckland, New Zealand URL: http://www.pacis-net.org/file/2007/1247.pdf [WebCite Cache]
25. Lu Y, Weichao WW, Bhargava B, Xu D. Trust-based privacy preservation for peer-to-peer data sharing. IEEE Trans Syst Man Cybern A 2006 May;36(3):498-502. [doi: 10.1109/TSMCA.2006.871655]
26. Almenarez F, Marin A, Campo C, Garcia C. Managing ad-hOC trust relationships in pervasive computing environments. 2004 Presented at: Proceedings of the Workshop on Security and Privacy in Pervsive Computing SPPC; 2004; Vienna, Austria URL: http://www.vs.inf.ethz.ch/events/sppc04/papers/sppc04_almenarez.pdf [WebCite Cache]
27. Jameel H, Hung LX, Kalim U, Sajjad A, Lee S, Lee YK. A trust model for ubiquitous systems based on vectors of trust values. : IEEE Computer Society; 2005 Presented at: Proceedings of the 7th IEEE International Symposium of Multimedia; 2005; Washington, DC, USA p. 674-679. [doi: 10.1109/ISM.2005.22]

28. Huang J, Nicol D. A calculus of trust and its application to PKI and identity management. : ACM; 2009 Presented at: Proceedings of the 8th Symposium on Identity and Trust on the Internet; Apr 14-16, 2009; New York, NY, USA p. 23-37. [doi: 10.1145/1527017.1527021]
29. Krukow K, Nielsen M, Sassone V. Trust models in ubiquitous computing. Philos Trans A Math Phys Eng Sci 2008 Oct 28;366(1881):3781-3793. [doi: 10.1098/rsta.2008.0134] [Medline: 18678555]
30. Ray I, Ray I, Chakraborty S. A context-aware model of trust facilitating secure ad hoc collaborations. In: Trust Modeling and Management in Digital Environments: From Social Concept to System Development. Hershey, PA, USA: IGI Global; 2010:250-281.
31. Mui L, Mohtashemi M, Halberstadt A. A computational model of trust and reputation for e-business. 2002 Presented at: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02), Volume 7; Jan 7-10, 2002; IEEE Computer Society, Washington, DC, USA p. 188.
32. Bertino E, Ferrari E, Squicciarini A. Trust-X: a peer-to-peer framework for trust establishment. IEEE Trans Knowl Data Eng 2004 Jul;16(07):827-842. [doi: 10.1109/TKDE.2004.1318565]
33. Chakraborty S, Ray I. p-Trust: a new model of trust to allow finer control over privacy in peer-to-peer framework. J Comput 2007 Apr 01;2(2):14-24. [doi: 10.4304/jcp.2.2.13-24]
34. Lederer S, Mankoff J, Dey AK, Beckmann CP. Report No UCB/CSD-3-1257. Berkely, CA, USA: University of California; 2003 Jul. Managing personal information disclosure in ubiquitous computing environments URL: http://www.cs.cmu.edu/~assist/publications/old-pubs/privacy-techreport03.pdf [WebCite Cache]
35. Friedewald M, Vildjiounaite E, Punie Y, Wright D. Privacy, identity and security in ambient intelligence: a scenario analysis. Telematics Informatics 2007 Feb;24(1):15-29. [doi: 10.1016/j.tele.2005.12.005]
36. Adams A, Sasse MA. Privacy in multimedia communications: protecting users, not just data. 2001 Presented at: Joint Proceedings of Human-Computer Interaction/Interaction d'Homme-Machine (IMH-HCI 01); 2001; Lille, France p. 49-64 URL: http://www.eis.mdx.ac.uk/ridl/aadams/hci01.pdf [WebCite Cache]
37. Jiang X, Landay AJ. Modeling privacy control in context-aware systems. IEEE Pervasive Comput 2002 Jul;1(3):59-63. [doi: 10.1109/MPRV.2002.1037723]
38. Kapadia A, Henderson T, Fielding J, Kotz D. Virtual walls: protecting digital privacy in pervasive environments. In: LaMarca A, Langheinrich M, Truong KN, editors. Pervasive Computing: 5th International Conference, PERVASIVE 2007, Toronto, Canada, May 13-16, 2007, Proceedings (Lecture Notes in Computer Science / Information ... Applications, incl. Internet/Web, and HCI). Verlag Berlin, Heidelberg: Springer-Verlag; 2007:162-179.
39. Diaz C, Seys S, Claessens J, Preneel B. Towards measuring anonymity. In: Privacy Enhancing Technologies: Second International Workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002: revised papers. New York: Springer-Verlag; 2003:54-68.
40. Lederer S, Mankoff J, Dey AK. Report No, UCB/CSD-2-1288. Berkeley, CA, USA: University of California; 2002 Jun. A conceptual model and metaphor of everyday privacy in ubiquitous computing environments URL: http://www.cs.cmu.edu/~io/publications/old-pubs/privacy-techreport02.pdf [WebCite Cache ID 6GtjlLKAH]
41. Dritsas S, Gritzalis D, Lambrinoudakis C. Protecting privacy and anonymity in pervasive computing: trends and perspectives. Telematics Informatics 2006 Aug;23(3):196-210. [doi: 10.1016/j.tele.2005.07.005]
42. Gray E, O'Connell P, Jensen C, Weber S, Seigneus JM, Yong C. Technical Report 66. Dublin, Ireland: Department of Computer Science, Trinity College; 2002. Towards a framework for assessing trust-based admission control in collaborative ad hoc application URL: https://www.cs.tcd.ie/publications/tech-reports/reports.02/TCD-CS-2002-66.pdf [accessed 2013-05-26] [WebCite Cache ID 6JgMifjco]
43. Kagal L, Berners-Lee T, Connolly D, Weitzner D. Promoting Interoperability Between Heterogeneous Policy Domains.: MIT Computer Science and Artificial Intelligence Laboratory; 2008. URL: http://www.w3.org/2006/07/privacy-ws/papers/32-kagal-rein/ [WebCite Cache ID 6GtjI1wdN]
44. Skopik F. Dynamic Trust in Mixed Service-oriented Applications (dissertation). Austria: Vienna University of Technology; 2010. URL: http://www.infosys.tuwien.ac.at/Staff/sd/papers/ [WebCite Cache ID 6Jg2qhzqu]
45. Joshi A, Finin T, Kagal L, Parker J, Patwardhan A. Security policies and trust in ubiquitous computing. Philos Trans A Math Phys Eng Sci 2008 Oct 28;366(1881):3769-3780. [doi: 10.1098/rsta.2008.0142] [Medline: 18672450]
46. Khiabani H, Sidek ZM, Manan JL. Towards a unified trust model in pervasive systems. : IEEE Computer Society; 2010 Presented at: Proceedings of the IEEE 24th International Conference on Advanced Information Networking and Applications Workshops; 2010; Perth, Australia p. 831-835. [doi: 10.1109/WAINA.2010.144]
47. Salah H, Eltoweissy M, Abel-Hamid A. Computational Trust for Peer-to-Peer Web Services.: Virginia Tech; 2008. URL: http://www.cs.purdue.edu/homes/fahmy/icnp2008/posters/Salah.pdf [WebCite Cache ID 6Jg36YwTi]
48. Pearson S, Mont MC. Sticky policies: an approach for managing privacy across multiple parties. Computer 2011 Sep;44(9):60-68. [doi: 10.1109/MC.2011.225]
49. Wang Y, Kobsa A. Privacy-enhancing technologies. In: Grupta M, Sharman R, editors. Handbook of Research on Social and Organisational Liabilities in Information Security. Hersey, USA: IGI Global; Dec 2008:203-227.
50. CEN. Analysis of Privacy Protection Technologies, Privacy-Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management Systems (IMS), the Divers Thereof and the Need for Standardization. Brussels: European

Committee for Standardization, CWA; 2005. URL: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/%20CWA15263-00-2005-Apr.pdf [WebCite Cache]
51. Lilien L, Bhargava B. A scheme for privacy-preserving data dissemination. IEEE Trans Syst Man Cybern A 2006 May;36(3):503-506. [doi: 10.1109/TSMCA.2006.871655]
52. Tschudin C. Apoptosis - the programmed death of distributed services. In: Vitek J, Jensen C, editors. Secure Internet Programming: Security Issues for Mobile and Distributed Objects, LNCS. Berlin: Springer; 1999.
53. Pallapa G, Kumar M, Das SK. Privacy infusion in ubiquitous computing. 2007 Presented at: Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services; Aug 6-10, 2007; Philadelphia, PA p. 1-8. [doi: 10.1109/MOBIQ.2007.4451030]
54. Kahl C, Böttcher K, Tschersich M, Heim S, Rannenberg K. How to enchance privacy and identity management for mobile communities: approach and user drive concepts of the PICOS project. In: Rannenberg K, Varadharajan V, Weber C, editors. Security and Privacy - Silver Linings in the Cloud: 25th IFIP TC 11 International Information Security Conference, SEC 2010, Held as Part of WCC 2010, Brisbane, Australia, September 2010 Proceedings. Berlin: Springer; 2010:277-288.
55. HL7 International, Inc. HL7 Privacy, Access and Security Services (PASS) Specification. Ann Arbor, MI, USA: HL 7 International; 2010. URL: http://wiki.siframework.org/file/view/PASS+Access+Control+Conceptual+Model+Release+1.0.pdf [WebCite Cache ID 6Jg5c7azV]
56. Hoaglund JA. Specifying and Implementing Security Policies Using LaSCO, the Language for Security Constraints on Objects (PhD dissertation). California, USA: University of California; 2000. URL: http://arxiv.org/ftp/cs/papers/0003/0003066.pdf [WebCite Cache ID 6JmSydaer]
57. Price BA, Adam K, Nuseibeh B. Keeping ubiquitous computing to yourself: a practical model for user control of privacy. Int J Hum-Comput St 2005;63(1-2):228-253. [doi: 10.1016/j.jhcs.2005.04.008]
58. Patwardhan A, Korolev V, Kagal L, Joshi A. Enforcing policies in pervasive environments. 2004 Presented at: The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004; Aug 22-26, 2004; Boston, USA p. 299-308. [doi: 10.1109/MOBIQ.2004.1331736]
59. Grimm S, Lamparter S, Abecker A, Agarwal S, Eberhart A. INFORMATIK 2004 – Informatik verbindet, Band 2, Proceedings of Semantic Web Services and Dynamic Networks. Germany: Gesellschaft für Informatik e.V. (GI); 2004. Ontology based specification of Web service policies URL: http://subs.emis.de/LNI/Proceedings/Proceedings51/GI-Proceedings.51-119.pdf [WebCite Cache ID 6JgB5Fvhi]
60. Cote PP. PC Expressions. 2004. Avoid distrust online URL: http://www.pcexpressions.net/Portfolio/Avoiding%20Distrust%20Online.pdf [WebCite Cache ID 6JgBjrW2R]
61. Gao F, He J, Ma S. Trust based privacy protection method in pervasive computing. J Netw 2012 Feb 01;7(2):322-328. [doi: 10.4304/jnw.7.2.322-328]
62. Louviere JJ, Hensher DA, Swait JD. Stated Choice Methods: Analysis and Applications. Cambridge, UK: Cambridge University Press; 2000.
63. Zuo Y, O'Keefe T. Post-release information privacy protection: a framework and next-generation privacy-enhanced operating system. Inf Syst Front 2007;9:451-467. [doi: 10.1007/s10796-007-9057-0]
64. Kumaraguru P, Cranor LF, Lobo J, Calo SB. A survey of privacy policy languages. In: Workshop on Usable IT Security Management (USM 07). 2007 Presented at: SOUPS '07: Proceedings of the 3rd Symposium on Usable Privacy and Security; Mar 2007; New York, NY, USA URL: http://precog.iiitd.edu.in/Publications_files/Privacy_Policy_Languages.pdf [WebCite Cache]
65. Damianou N, Bandara A, Sloman M, Lupu EC. A Survey of Policy Specification Approaches, Technical Report. London, UK: Imperial College of Science Technology and Medicine; 2002. URL: http://www.doc.ic.ac.uk/~mss/Papers/PolicySurvey.pdf [WebCite Cache ID 6JgKPou7m]
66. Karjot G, Schunter M, Waidner M. Platform for enterprise privacy practices: privacy-enabled management of customer data. Berlin: Springer-Verlag; 2003 Presented at: 2nd Workshop on Privacy Enhancing Technologies (PET 2002), LNCS 2482; Apr 14-15, 2002; San Francisco, CA, USA p. 69-84.
67. Kagal L, Finin T, Joshi A. A policy language for a pervasive computing environment. Los Alamitos, CA, USA: IEEE Computer Society; 2003 Presented at: IEEE 4th International Workshop on Policies for Distributed Systems and Networks; Jun 4-6, 2003; Lake Como, Italy p. 63-74. [doi: 10.1109/POLICY.2003.1206958]
68. Blobel B. Ontology driven health information systems architectures enable pHealth for empowered patients. Int J Med Inform 2011 Feb;80(2):e17-e25. [doi: 10.1016/j.ijmedinf.2010.10.004] [Medline: 21036660]

Abbreviations

DS: data subject
PHI: personal health information
PII: personal identifiable information
TA: trust authority
TC: trust calculator

Edited by G Eysenbach; submitted 26.05.13; peer-reviewed by M Rigby, M Rogers, D Willison; comments to author 18.06.13; revised version received 23.07.13; accepted 29.08.13; published 08.10.13

Please cite as:
Ruotsalainen PS, Blobel B, Seppälä A, Nykänen P
Trust Information-Based Privacy Architecture for Ubiquitous Health
JMIR Mhealth Uhealth 2013;1(2):e23
URL: http://mhealth.jmir.org/2013/2/e23/
doi:10.2196/mhealth.2731
PMID:

Original Paper

Privacy-Related Context Information for Ubiquitous Health

Antto Seppälä, MS Comp Sc; Pirkko Nykänen, PhD; Pekka Ruotsalainen, DSc (Tech)

Center for Information and Systems, School of Information Sciences, University of Tampere, Tampere, Finland

Corresponding Author:
Antto Seppälä, MS Comp Sc
Center for Information and Systems
School of Information Sciences
University of Tampere
Kanslerinrinne 1
Tampere, 33014
Finland
Phone: 358 407069919
Fax: 358 32191001
Email: Antto.Seppala@uta.fi

Abstract

Background: Ubiquitous health has been defined as a dynamic network of interconnected systems. A system is composed of one or more information systems, their stakeholders, and the environment. These systems offer health services to individuals and thus implement ubiquitous computing. Privacy is the key challenge for ubiquitous health because of autonomous processing, rich contextual metadata, lack of predefined trust among participants, and the business objectives. Additionally, regulations and policies of stakeholders may be unknown to the individual. Context-sensitive privacy policies are needed to regulate information processing.

Objective: Our goal was to analyze privacy-related context information and to define the corresponding components and their properties that support privacy management in ubiquitous health. These properties should describe the privacy issues of information processing. With components and their properties, individuals can define context-aware privacy policies and set their privacy preferences that can change in different information-processing situations.

Methods: Scenarios and user stories are used to analyze typical activities in ubiquitous health to identify main actors, goals, tasks, and stakeholders. Context arises from an activity and, therefore, we can determine different situations, services, and systems to identify properties for privacy-related context information in information-processing situations.

Results: Privacy-related context information components are situation, environment, individual, information technology system, service, and stakeholder. Combining our analyses and previously identified characteristics of ubiquitous health, more detailed properties for the components are defined. Properties define explicitly what context information for different components is needed to create context-aware privacy policies that can control, limit, and constrain information processing. With properties, we can define, for example, how data can be processed or how components are regulated or in what kind of environment data can be processed.

Conclusions: This study added to the vision of ubiquitous health by analyzing information processing from the viewpoint of an individual's privacy. We learned that health and wellness-related activities may happen in several environments and situations with multiple stakeholders, services, and systems. We have provided new knowledge regarding privacy-related context information and corresponding components by analyzing typical activities in ubiquitous health. With the identified components and their properties, individuals can define their personal preferences on information processing based on situational information, and privacy services can capture privacy-related context of the information-processing situation.

(JMIR Mhealth Uhealth 2014;2(1):e12) doi:10.2196/mhealth.3123

KEYWORDS

ubiquitous health; privacy; context information; trust; policy

Introduction

Overview

Ubiquitous computing makes it possible to collect all kinds of data anywhere and anytime [1] and allows integration of health care delivery and services into people's everyday lives [2,3]. This paper builds on a conceptual framework [4] in which ubiquitous health is defined as an open and dynamic ubiquitous information space. The space is presented as digital systems that consist of one or more information systems, their stakeholders, and environments. These systems create a dynamic network that offers and provides services to citizens. In the information space, individuals and service providers can select, tailor, and combine services and systems that belong to the network. To enable access to personal information, individuals and providers need to discuss trust, privacy level, and proffered service.

Ubiquitous health services can be offered by providers that are licensed and regulated by medical ethical codes and health care–specific legislation and other juridical norms and by actors that are not affected by health care–related regulations. To separate these two groups, we divided them as regulated health care services and other services. Providers offering regulated health care services have strict defined responsibilities and obligations concerning service provision, care, professionals, documentation, and information processing. There are also general regulations on privacy and security requirements (eg, data protection and processing directives) and business domain–specific regulations. Regulations cover laws; norms; good practice guidelines; and other rules controlling, constraining, or limiting activity of participants. These regulations can affect ubiquitous health services but they often do not meet the challenges of technological innovations well.

In ubiquitous health, trustworthiness and privacy are key challenges [4-6]. There are privacy threats created by autonomous and hidden processing of information and rich contextual metadata. There is no predefined trust between participants, and the business objectives, needs, interests, and policies of stakeholders may be unknown to the individual [4]. Information in ubiquitous health is highly sensitive and confidential, and the existence of services and actors that are not strictly regulated by health care-specific legislation creates threats and risks for individual privacy. In addition, information processing can happen in multiple systems and situations with different regulations, and risks of secondary use exist. The lack of predefined trust and privacy risks emphasizes the importance of an individual's ability to control his or her privacy.

For trusted information processing in ubiquitous health, we follow the principles presented in Ruotsalainen et al [4] and according to them, an individual should have the right to verify dynamically the trustworthiness of the ubiquitous health network and any system that requires or processes the individual's personal information for secondary purposes; control personal health information processing, inside systems and between them; be notified of all situations and contexts in which personal information is collected, processed, stored, and/or disclosed; and create situation-specific, context-aware, and granular personal privacy and trust policies, which control how personal information is collected, processed, disclosed, shared, stored, or destroyed.

Systems and stakeholders should have the responsibility to ensure trust verification by publishing their privacy policies and environmental and contextual features; openness of interests, business needs, and policies as well as their relationships with other systems; and transparency of information processing.

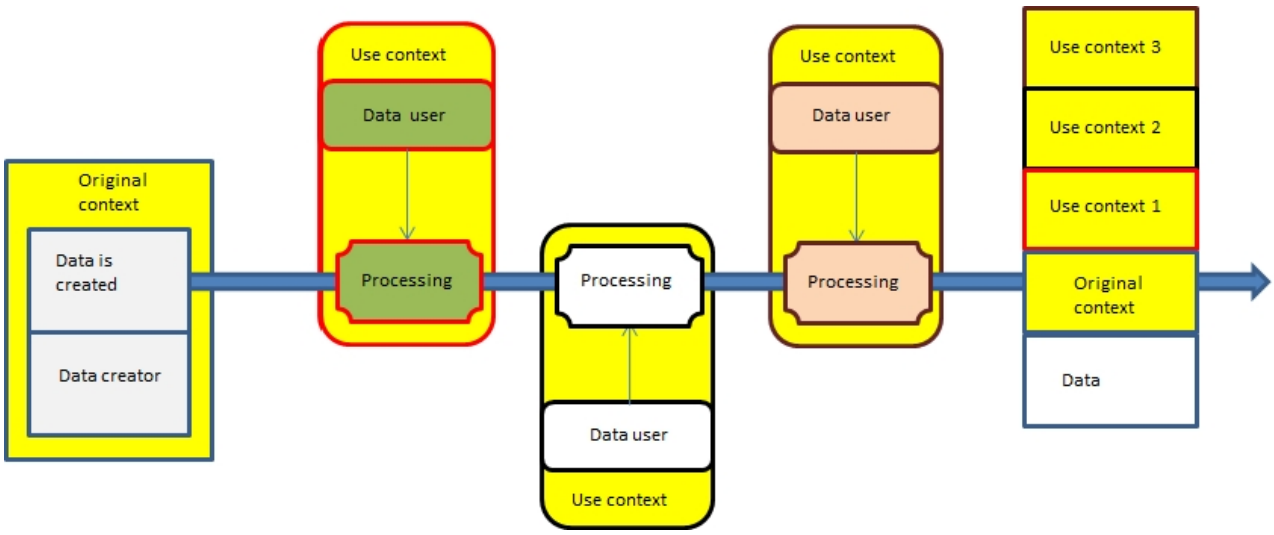
To protect his or her rights, an individual needs information about privacy, that is, privacy attributes, to define his or her personal privacy preferences. Privacy attributes enable privacy to be a concrete issue for individuals. In Nykänen et al [7], we defined privacy attributes as benefit, benevolence, capability, competence, confidence, context, reliability, and value. Privacy attributes and their contents have not generally been researched widely. The focus in this study is the context attribute, which refers to the situation in which data are created or processed. The objective is to analyze and define privacy-related context information components and their corresponding properties.

When data are created, a continuum of data is born. During the different processing situations, data or its properties may change. Original context refers to a situation when data are created. In various use contexts and processing situations, context information is incrementally created and it describes the current context and enables tracking of the context history. Thus, data have embedded context information that can be used by privacy services for trust calculation and to decide whether processing is allowed (Figure 1).

An individual's privacy preferences can be implemented with adaptable privacy policies. In previous work [8], we concluded a formula for privacy policies to contain (1) trust information that is a value of a system- or environment-specific calculation of regulatory compliance and trustworthiness; (2) sensitivity of the data; (3) situation of the information use; and (4) purpose of the data collection or use.

Policy formulation is a decision process in which an individual selects privacy rules and services and how much information can be traded compared to the offered service and the level of privacy attributes. In this study, our hypothesis is that context information enables formulation of context-aware privacy policies hence enabling trustworthy processing of personal health and wellness information and realizing individuals' rights for privacy in ubiquitous health. In Ruotsalainen et al [8], we presented a privacy architecture that could use context information in trust calculation and in context-aware privacy policies to control an individual's personal information. With this study, we add knowledge to our earlier research by studying the privacy-related context information and by defining the corresponding components and their properties that support privacy management in ubiquitous health.

Figure 1. Data continuum and context information.



Prior Work

Privacy and Trust

Privacy refers to an individual's ability to control information about him- or herself [9]. Privacy is a very personal concept and dependent on the context, because it may vary among jurisdictions, cultures, economies, time, and individuals [10-12]. Smith et al [13] claim that privacy is so bound to the specific context that it cannot be conceptualized as a single and unambiguous concept; rather it should be treated as a set of interests. Clarke [14] argues that it is useful to understand privacy as the interest of keeping personal space free from inference and has divided privacy into four dimensions: person, personal behavior, personal communications, and personal data. Information privacy means that personal information should not generally be available to other persons or organizations and an individual should have major control or influence over the personal data controlled by others and its use [14]. In this research, we refer to privacy as an individual's personal view within the legislative boundaries.

Trust is a concept closely related to privacy, and usually, the higher the value of trust, the lower the need for privacy [4]. Trust implicates the willingness to share personal information with others [15]. Schoorman et al [16] emphasize that trust is based on a relationship and the level of trust expresses the level of risk an individual is willing to take. Abdul-Rahman and Hailes [17] have defined three characteristics of trust: (1) trust is subjective, (2) actions we cannot monitor affect trust, and (3) trust level is dependent on how others' actions affect our actions. Several trust models has been developed for calculating trustworthiness [16,18-20].

Ubiquitous computing systems should be open and dynamic, because pre-identification of participants is impossible and they might change regularly [21]. In these kinds of distributed environments, collaboration is vital because multiple systems together try to achieve goals and perform tasks and it is crucial for systems to know which entities they should or should not interact with [22]. Traditional privacy and security solutions are not adequate for ubiquitous environments because there is no central control or predefined users or policies [19,21,23]. Privacy and security architecture and decisions need to be based on trust and its properties [19,21,24].

Context and Context Awareness

Context has been mostly defined with user profile, user emotion, and user location and identities of nearby people and objects and changes to those objects [25-28]. According to Dey et al [29], the three most relevant entities are places, people, and things. These entities have to be considered from different viewpoints such as location, activity, and identity. Dourish [30] proposes that context and content cannot be separated; the context arises from the activity itself and it cannot be an external description of the setting. He claims that context is a relational, interactional property between objects and activities and the scope of features must be defined dynamically [30]. Dey and Abowd ([28], pp. 3-4) defined context as: "Context is any information that can be used to characterize the situation of an entity. An entity is an individual, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves."

This definition is open and it considers that any information that is relevant for information processing in a situation can be used as a context. Context information can, for example, be information about the user, device, environment, or situation. Thus, it is meaningful to talk about context related to something that exists. There are three main uses for context information [29]: (1) presenting information and services to a user or using context to propose actions to be performed, (2) execution of a service automatically on behalf of the user, and (3) applications can tag context to information for later retrieval.

In context-aware computing, applications and systems are able to perceive their surroundings and environment, adapt according to the context, and perform autonomously. Context awareness refers to adaptability, which means that applications and systems exploit perceived context information and adapt their behavior accordingly [31]. In this view, context information is information that enables behavior modification based on this information and its relations. The systems, applications, and entities have to define the scope themselves.

According to Viswanathan et al [32], the key point for successful ubiquitous health is context awareness, and there are already several context-aware applications in the health and wellness domain. A lot of research has been done to support personalized actions and services in home care, chronic disease management, and ambient assisted living [33-37] with different personalized health status, body sensor networks, activity or behavior monitoring, decision support, and reminder applications [32,33,35-40]. In the hospital environment, many professionals are very agile, and context-aware technologies may help by personalizing services for them by location, time, and social context [41]. According to previous studies [33,42], there are several experiments on context-aware computing that have been created in hospital environments to improve patient record management, communication among professionals, and information sharing by including context awareness in patient room equipment.

Policies

In ubiquitous environments, privacy requirements can be expressed with policies. Privacy policy can be understood as a personal statement on privacy. With policies, individuals can set computational rules explicitly stating their personal privacy preferences on how their information can be processed, used, disclosed, and shared [21,43,44]. Policies are typically expressed with a policy language [45]. To enable personal privacy policies with computational rules requires definition of privacy attributes. Privacy policies can be implemented with setting values on privacy attributes. Context-aware policies based on context information enable dynamic adaptation of privacy control strategies and tailored privacy decision support services. A technique called sticky policy enables attaching policies into data to ensure that data are processed according to an individual's wishes [44].

Behrooz and Devlic [46] propose a context-aware privacy policy language based on two design considerations: (1) situations and privacy rules are defined separately, and (2) a context requestor can be specified based on its identity or social relationship to a user. These principles mean that privacy policies are set for different situations. Ghosh et al [47] presented a semantically rich policy-based system that can reason on user's context and thus protects a user's privacy dynamically during runtime. Schaub et al [23] presented a privacy context model with three major entities—user, user's environment, and user's activities. Their model takes into account information, physical, and territorial aspects of privacy. Blount et al [48] proposed a context-dependent policy model in which field context contains information when conditions for the policy are valid. These values may be from either the subject or the requestor.

Methods

Scenarios and User Stories

Scenarios are means to describe the system's intended usage. Scenario-based design techniques produce descriptions of how people do things and how they can accomplish different tasks with the system. With scenarios, designers can find new ways of doing things and new things to do. Scenarios capture goals, entities, behavioral information (eg, actions, activities, and events) and what people are trying to accomplish with the system [49,50]. They can also describe different related actors with their own objectives. Typically, scenarios have a plot that consists of several events, things that happen during activities, changes in the setting, etc. Scenarios are work-oriented analysis methods; thus, they are suitable for our purposes, because we are analyzing typical activities of an individual in an ubiquitous health environment to recognize the needs for context information.

In our previous articles, we analyzed privacy threats and the principles for trusted information processing [4], defined privacy attributes [7], and analyzed the requirements for information that should be used in privacy policy formulation and common threats and challenges concerning privacy in ubiquitous health [8]. Our previous results created the framework for the scenario development and analyses and for the requirements for context information. In this research, we created scenarios that were based on materials collected in our earlier empirical research on personal wellness [51-53] performed with focus groups and literature studies focusing on health and wellness activities and technical applications on chronic disease management, self-health management, ubiquitous health, and wellness approaches. Scenarios were designed to capture the characteristics of different situations, such as a general wellness management situation without any specific needs and a specific setting with a chronic disease. With scenarios, we could identify a wide selection of typical activities in ubiquitous health.

We first created two textual scenarios describing the main actors, their backgrounds, and current health and wellness situations and next, we determined the main goals, activities, and entities. Then, we further divided both scenarios into 10 user stories that described in more detail the activities and services the individuals needed in their situations. Each user story focuses on 1 activity of a scenario and it is a short textual and informal description of a user case. Because context arises from activity [30] with the user stories, we could capture activities in ubiquitous health to identify information-processing situations and privacy-related context information.

At first, scenarios described typical wellness approaches emphasizing services that are not regulated by health care regulations, for example, lifestyle management and health-related behaviors. The objective was to recognize activities and entities outside regulated health care services. Then we approached chronic disease management scenarios with a focus on identifying collaboration between regulated health care services and personal attempts to manage health outside the provider networks with other services. These scenarios were analyzed to recognize activities and information-processing situations. To summarize, these scenarios helped us to analyze the aspects of two different situations in ubiquitous health: (1) ubiquitous health without regulated health care providers' participation; and (2) ubiquitous health with regulated health care, for example, service portfolio is a combination of services produced by a regulated health care provider(s) and other health and wellness providers.

An Example Scenario

As an example, we present the following scenario. Peter is a 23-year-old healthy student who begins to feel tired and ill and he decides to seek help from student health services. After a few tests and doctor visits, Peter is diagnosed with type 2 diabetes mellitus. From now on, Peter has to pay attention to his habits and choices concerning healthy living for the first time in his life. We divided this scenario into more detailed user stories describing activities related to chronic diseases in a ubiquitous health environment. In Table 1, we present an example analysis of a user story. In Table 2, we present a detailed example of a single activity in ubiquitous health with its related privacy concerns, Peter's policies, and the context information that a policy example requires.

Table 1. An example analysis of a user story in chronic disease scenario. User story 2.1: Peter receives a medical device with sensors to manage and care for his disease and automatically measure and monitor his condition. Devices can also automatically inform his doctor about the results and major changes.

Role	Individual and information controller with rights for privacy, to control processing and secondary use of information. Peter can decide who can access data created by the device. Peter needs privacy policies to control his own personal health system (PHS) use and the information it contains.
Activities	Data is created in the sensors and transferred to PHS. PHS analyzes the information and compares it to past information. PHS informs Peter's doctor about a major change in a value. Doctor accesses the information and makes a medical decision.
Environment	Anywhere. No health care–specific regulations concerning the environment. Information sharing is based on Peter's known consent and privacy policies. All information created by the certified device is trusted. The device is regulated by specific legislation (eg, the European Union directive on medical devices). In case of a major change in measurement information, regulated health care service will participate and then the environment will be strictly regulated by health care–specific regulations.
Information systems	Medical device, Peter's own PHS and possibly electronic health record system. Sensor and measurement data is stored in PHS and Peter's health records are in regulated electronic health record system. Peter has total control over his PHS.
Stakeholders	Peter, medical device, PHS, and licensed medical professional (doctor) with responsibilities concerning care and patients privacy
Services	Certified medical device measuring blood sugar levels PHS diabetic information analysis Regulated health care service activated by Peter's PHS in case of a major change in Peter's measurement values
Information content	Measurement and monitoring data from sensors and medical device Health and wellness information in PHS is controlled by Peter. The medical information is regulated in health care organization's electronic health record system.
Original context of the information	Information is created by a certified medical device controlled by Peter. The environment does not have any specific domain regulations. Information is in Peter's control and he has full rights for it. Peter's personal context-aware privacy policies are the main source for limitations and constraints on information processing.
Requirements for context properties	Peter's PHS is a trusted information system in his control so it has full processing rights and can activate other services if needed following Peter's privacy policies. Peter has defined in his policies that different measurement and sensor data is very sensitive and sets limitation for what purpose information can be used. In other cases, PHS cannot grant access to information without Peter's authorization. Other than regulated health care, services have to share their principles for information processing, security and privacy policies, and for what purpose they want to process the information.

Table 2. An example analysis of an activity: data is created in the sensors and transferred to the PHS.

Privacy challenges and threats [8]	Peter's policies	Required context information for policy 1
Lack of awareness	1. Peter thinks that this kind of data is highly personal and can only be accessed automatically by a health care professional participating in Peter's care service.	Situation: activity, processing type, actor, target, information sensitivity, and purpose for processing
It is difficult to know how data is used in the future	2. To use the data, transparency of processing is needed; therefore, the provider has to publish detailed privacy and security policies and allow third-party auditing.	Environment: general privacy and security regulations, location, and society
Relationships between systems may be unknown	3. To prevent secondary use, copying data is not allowed. If copying is required, Peter has to be notified and his known consent is required.	Service: type, role, provider, location, and objective
Potential secondary use of information	4. Health care professionals are not allowed to disclose data without Peter's known consent.	Individual: role, rights to control information, relation to the activity, confidentiality requirements
Users want to control how systems use personal health information		Stakeholder: identity, type, role, purpose, and justification for processing
How to guarantee that data is processed following the legal constraints and according to the individual's policies		IT system: identity, type, controller

Results

In an open and dynamic ubiquitous health information space, there are no possibilities to predefine entities or activities and most aspects of information processing are dynamic. In the scenarios and user story analyses, we recognized how different activities are reasons for information-processing situations in ubiquitous health, how several entities can create and use information, and how the same information can be used later to support different activities. In addition, scenarios showed that activities could happen autonomously with information systems even without human participation; for instance, based on some measurement of vital signs or monitoring of data. Thus, information processing happens because some entity performs an activity in a certain environment. Situation describes this occurrence and therefore is chosen as the core component defining privacy-related context information. It is linked to a certain activity; that is, the reason for information processing. Context information needs to include the whole situation and all participants because of the dynamic nature and limitations in predefining activities and stakeholders in ubiquitous health.

As a result of our scenarios and user stories, we present the two kinds of basic models for ubiquitous health: ubiquitous health without regulated health care providers, and ubiquitous health with regulated health care service providers.

The first case is an open environment with multiple entities with different kinds of domain environments and interests. All participants are by definition untrusted. Health care–specific regulations do not apply, but regular privacy and security legislations set limitations for information processing. In addition, different domains may have their specific legislations (eg, social care, wellness services, medical devices, or pharmacy). Environment and entity-specific regulations and an individual's personal context with privacy preferences are necessary for adaptable privacy policies. An individual's role, environment, and privacy requirements may vary between used services or information systems and information sensitivity influences heavily on personal policies. An individual's rights to control data and information must be discussed with service providers.

In the second case, there are also entities that are affected by health care–specific regulations. Depending on who or what provides service and/or controls information, there might be strict health care–specific regulations for service provision, organizations, professionals, information systems, and information processing. Regulated health care services are to some extent trusted and privacy threats and risks occur especially when information is transferred from them or processed beyond their authority. It is very critical to capture who is responsible for what, where and how services are provided, what information and sources are used, how sensitive the information is, and who controls participating information systems.

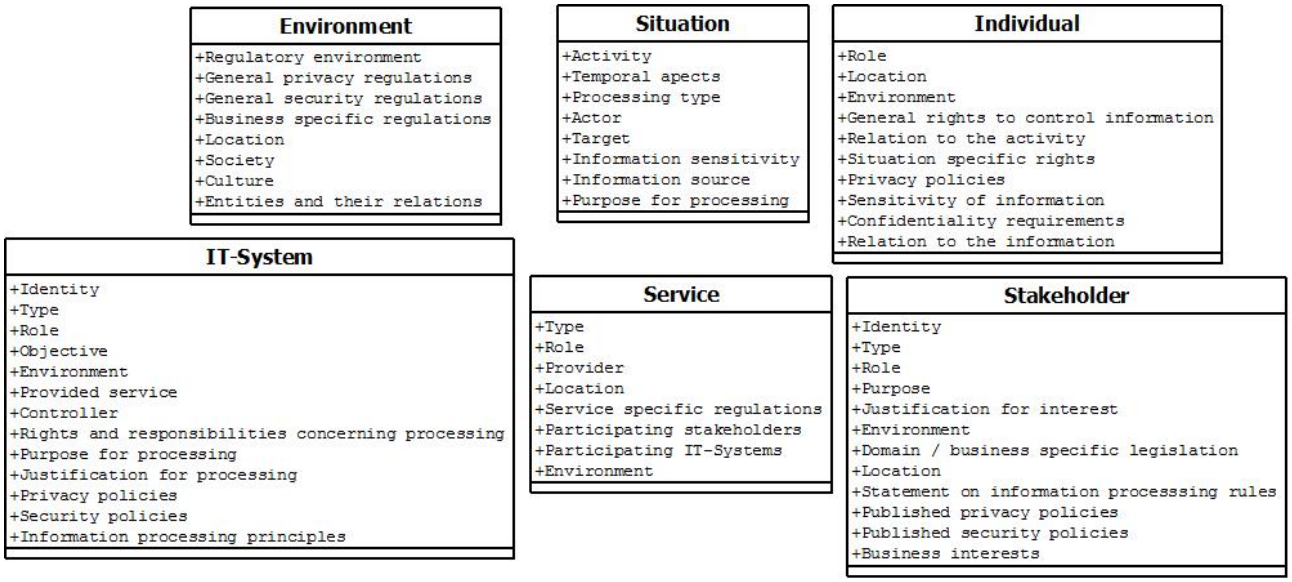
In a previous study [4], we defined ubiquitous health to be composed of services, information systems, stakeholders, and their environments. In addition to these, we have to capture the contexts of the information-processing situation and its object and/or subject. We should capture the following components and their properties on privacy, regulations, and requirements for trusted information processing: what happens (situation); who is the subject or the object (individual); what services are related to the situation (service); where this situation happens (environment); what social actors are active in the situation (stakeholder); and what computational entities participate (IT system).

In this research, the properties of the privacy-related context information components and their properties are derived by combining the results of the scenario analyses and the principles and requirements presented in the earlier research. We analyzed the results of the scenario analyses to explicate concrete properties for our components. In the example, we derived the context information that is needed to fulfil the requirements for

policies and to minimize known privacy threats. In this example, policy 1 in the Table 2 means that Peter sets a general policy that data created by sensors is highly sensitive and can only be automatically accessed by health care professionals participating in his care. Peter has total control over his data and the future use of data is based solely on Peter's wishes. The situation occurs when a regulated health care professional tries to access Peter's data to support Peter's care and to follow his condition. To manage his privacy, Peter needs information about the data user's environment and processing wishes. If parties other than a health care professional in Finland taking part in Peter's care service want to access the data, Peter's known consent is required. The data user is a regulated health care professional in Finland; that is, predefined as somewhat trusted and he/she can use the information only to make medical decisions and to follow Peter's condition. The data can only be accessed within Peter's PHS and the data cannot be copied or distributed. From the example, we can see how Peter needs several kinds of context information to create the example policy.

From the scenario analyses, we have defined the properties that are needed to fulfil the principles of trusted information processing and requirements set for privacy formulation concerning context information (Figure 2).

Figure 2. Privacy-related context information components and their properties for ubiquitous health.



A situation describes information processing that happens in a certain context because of some activity and by/for a certain individual. From the scenarios, we learned that environments might vary a lot; therefore, we need to understand the environment where the situation happens and component-specific environments (eg, individual, services, stakeholders, and IT systems) to capture all privacy aspects. With the environment, we do not only mean location and other position-based information, but especially important is to capture the type of environment. We have to perceive the properties of environment such as privacy, security, trust-related information, and information-processing rules and responsibilities. Regulations may differ a lot between environments and different businesses are affected by their specific legislation. Capturing environment is crucial because technological advancements such as cloud computing and big data create new types of privacy risks. For example, if a service is offered in the European Union but the data are stored or processed in an information system located in the United States, there are differences in legislations concerning privacy, security, or secondary use of data. People should be able to control where and why their data are processed.

An individual component describes the actual subject and/or object of health and wellness activities in ubiquitous health. It is linked differently to situations; an individual can create them, participate in them, and/or is an object. Properties needed from the individual are the role he/she has in the situation, location, and environment and what relation he/she has with the activity. Also, an individual's rights for controlling information processing (eg, content, disclosure and access to information), privacy policies, sensitivity and confidentiality requirements and what is his/her relation (eg, owner, controller, or subject) to information should be acknowledged. All these things affect how and on what basis systems can process information.

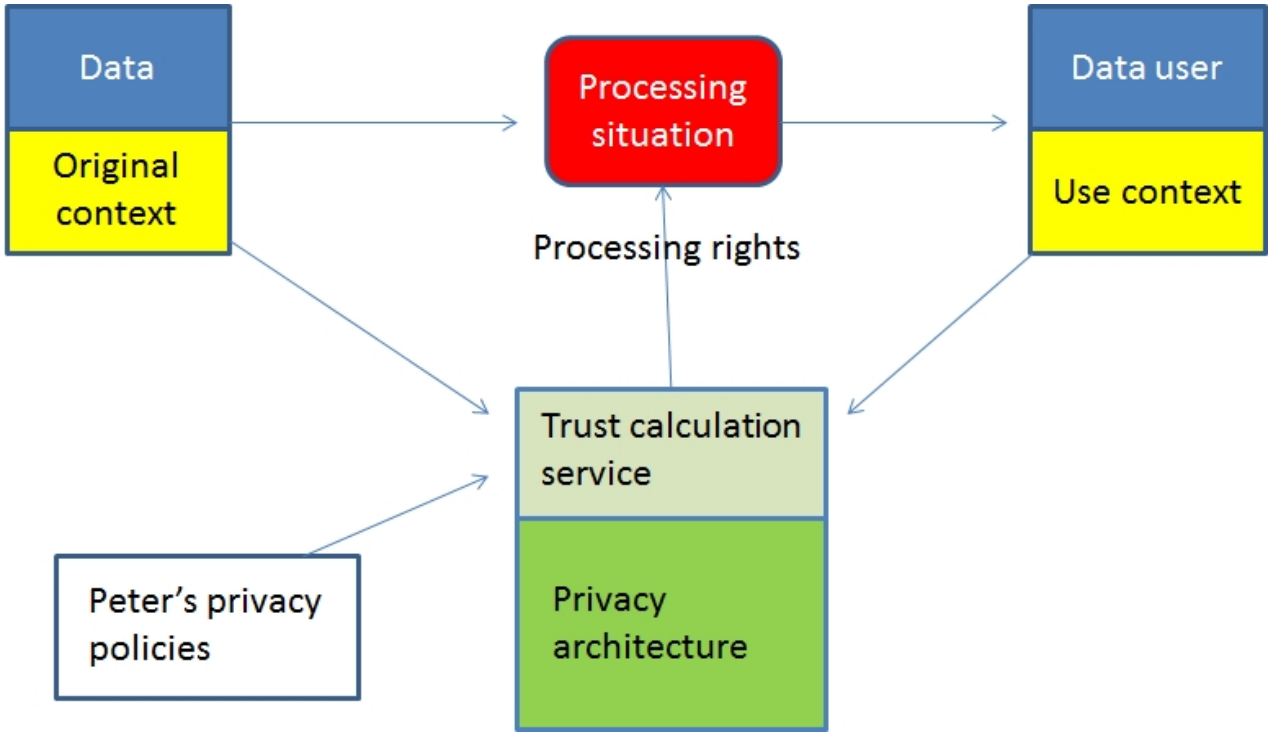
A service component describes regulated health care services and/or other services that can be offered by IT systems and/or stakeholders. An IT system component refers to all computational entities, which can include health information systems, personal health systems, ubiquitous systems, devices, sensors, etc. IT systems should be open about their processes and publish their privacy and security policies including how an individual's privacy is protected, relevancy of processing and actual data protection specifications, and detailed information-processing principles. This would improve transparency of information processing and increase trustworthiness. If an IT system does not publish necessary information, this has to be captured in the context information. Because information processing can happen anywhere, it is vital to capture its context because there are several characteristics affecting privacy that may differ between IT systems; for example, type, location, or regulative background. For example, there are big differences in regulations among information

systems, regulated medical devices (eg, have to be certified), and wellness devices. Stakeholder is the social component describing organizations and possible human participants. They can be actors or interested parties in a situation. They offer, participate, or are interested in services offered to individuals.

Our components can be used to increase trustworthiness of information processing because privacy policies can be adaptable and based on constraints, limitations, rules, rights, and responsibilities set with situational information. Components can also be used to analyze that the information processing follows the preferences set by an individual's privacy policies and the requirements from the original context of the information. For example, in our user story Peter may disclose medical and lifestyle data to a service provider to receive a selected service. Peter has set privacy policies using privacy properties. Before disclosure, Peter (his privacy architecture) needs the context information from the service provider to calculate if processing is according to the requirements set by Peter's own context-aware privacy policies and the original context of the information. Privacy architecture can then confirm that the use context is valid according to Peter's personal preferences and allow access to the information (Figure 3).

Our hypothesis was that privacy-related context information could be used to formulate context-aware privacy policies hence enabling trusted processing of personal health and wellness information. In this study, we analyzed contents of a privacy attribute context and presented components and their properties that can be used as part of privacy policies by setting situational constraints and limitations. These characteristics are also needed to capture information-processing contexts from the privacy perspective. All components or properties are not necessarily needed in all situations. In addition, if some systems refuse to cooperate in publishing context information, this has to be captured and acknowledged.

Figure 3. The use of privacy-related context information in ubiquitous health.



Discussion

In this research, we present an approach using privacy-related context information for privacy protection in ubiquitous health. Privacy is a business-enabler because individuals will not use these services if they cannot manage their privacy and trust. People need simple tools to manage their privacy and we have started this by defining the components situation, environment, individual, service, stakeholder, IT system, and their properties. These components describe the crucial privacy-related context information needed to improve trustworthiness of ubiquitous health. We present new knowledge by defining context, which is one of the main privacy attributes used in privacy policy definition. The results of this study can be used as a basis to create more formal models defining privacy-related context information in a computer-understandable format. Our results are in line with the preferred privacy level model by Lederer et al [11] but we have taken it a step further and divided context into original and use context and defined more detailed and concrete properties that could be valued and measured and used by privacy architecture for trust calculation.

Ubiquitous health is still an emerging field combining highly regulated health care with personal health and wellness services and systems. In health care, legislation and regulations define what privacy is and what kind of rights individuals have; that is, privacy is a state-defined property. Considering services and systems outside the regulated health care privacy is a personal property of an individual; that is, free will. The individual has the right to choose the use of his/her information and define policies as to how, where, and to what extent the information can be processed. In ubiquitous health, a privacy model is a combination of these two models and can be controlled with

policies. Policies can be personal preferences or defined by regulations. Using the scenarios, we could identify situations outside regulated health care to recognize requirements and characteristics of ubiquitous health. With organization-centric health care processes or workflows, we cannot really model ubiquitous health as a whole because there are many services and systems without predefined and regulated processes or workflows.

In ubiquitous health, service provision is based on customer relationships and trading on benefits of services against reducing personal privacy. Individuals should be able to verify the trustworthiness of service providers and decide if they are prepared to disclose personal information and reduce privacy. Because services are often offered as distributed, personalized and even autonomous, the privacy architecture should offer automatic privacy services and adapt dynamically to the situation. Scenarios and user stories showed that ubiquitous health is multidimensional with limitations of predefining situations. The amount of information needed and created in these situations can be huge, and the content and its sensitivity vary depending on the activity performed. Ubiquitous health is an open, dynamic, and collaborative environment and privacy needs to be based on trust and its properties [19,21,24].

In health care, privacy is mainly protected with access control and consent management. Access control is merely one tool to protect privacy. Managing privacy in ubiquitous health is a much broader issue than just controlling health care professionals' access to data. Access control with predefined rights, roles, and consents cannot really function because there is no central control or necessarily predefined processes, situations, or actors. To ensure privacy in ubiquitous computing, access control should be dynamic because of multiple changing entities. Context information enables dynamic management of rights [54]. Consent is an example of a personal policy but in ubiquitous health, policies are needed to cover several different situations that are more complex than those that consents are designed for. Policies have to be dynamic and context-aware. Corradi et al [55] present a dynamic and flexible security middleware that uses context as a basic concept in security policy specification and permissions are linked to the contexts instead of user identities or roles. Most research on privacy of context-aware computing focuses on capturing user's context or certain actors and using that information to adapt to privacy preferences [23,47,54].

In this study, we followed the approach of Behrooz and Devlic [46] to separate situations and privacy rules. We identified the necessary information to capture privacy aspects in information-processing situations. Then, privacy architecture can capture the situation and the conditions where data are created; that is, the original context and combine that with individual's policies and control future use contexts such as how, where, and by whom the information can be used. Our approach needs information from participating systems and currently its availability depends on the goodwill of participants. Additional to this information, privacy architecture can use external sources for estimating trustworthiness of systems (eg, recommendations from others, history, trust values, and trust calculations).

In the European Union, organizations are required to inform individuals about use of their data and publish privacy policies that should be comprehensive with high-level descriptions of their privacy practices [43]; however, these are not enough to safeguard individuals' rights. These privacy policies do not generally consider how data are actually processed after collection. So, one of the main challenges in privacy protection is how to enforce all relevant parties to explicate their detailed privacy policies [43]. Current legislation is not fully prepared to handle privacy threats of ubiquitous computing and does not obligate organizations to disclose their detailed privacy policies or information-processing principles. In the future, legislation needs to include the needs of privacy, citizens' rights, and ubiquitous computing. Citizens have to be able to control processing and secondary use of their personal information. Future privacy principles and norms need to progress from high-level principles to detailed regulations concerning the processing and use of information. This would bring openness and transparency to information processing and new kinds of responsibilities for organizations and informed rights for citizens. In addition, authorities or certificate organizations should be able to audit providers and offer recommendations about their trustworthiness.

The components defined in this research may have some limitations and may not be conclusive; however, based on the scenario analyses these are needed. In addition, some properties are hard to define explicitly or in measurable format. They have to be analyzed in more detail and formal models are needed to implement them in computational format. Also, we need more detailed analysis of what organizations should publish about their processes and privacy and security policies and principles. To create context-aware privacy services and policies in practice, we need to develop ontologies that explicate components, properties, and requirements that we have presented in this research. Ontologies are formal representations and should cover different activities, services, IT systems, stakeholders, information content, and especially relevant regulative environments. With ontologies, we can create computational rules that can be used to enforce regulations and personal policies into ubiquitous applications.

Because it is practically impossible for individuals to evaluate the trustworthiness of a system, and to understand detailed privacy and security requirements and set personal policies, we developed trust-based privacy management architecture for ubiquitous health [8]. This architecture model describes what privacy and security services are needed to enable trusted information processing in ubiquitous health. The architecture will apply privacy-related context information to create privacy and security policies that will ensure that information processing will not happen against the wishes of the individual and the original context of the data. The architecture contains decision support and policy services for individuals to help them define personal policies. This research adds to the architecture model by defining the required privacy-related context information components and their properties that are needed to create implementable tools and means for individuals to manage personal information privacy.

Acknowledgments

We acknowledge funding of the Trusted eHealth and eWelfare Space (THEWS) research project by the Finnish Academy of Sciences in the MOTIVE Research Programme during 2009–2012. The first author acknowledges the support of the Tampere Doctoral Programme in Information Science and Engineering (TISE).

Conflicts of Interest

None declared.

References

1. Varshney U. Pervasive healthcare and wireless health monitoring. Mobile Netw Appl 2007 Jul 12;12(2-3):113-127. [doi: 10.1007/s11036-007-0017-1]
2. Korhonen I, Bardram JE. Guest editorial: introduction to the special section on pervasive healthcare. IEEE Trans Inf Technol Biomed 2004 Sep;8(3):229-234. [Medline: 15484426]
3. Arnrich B, Mayora O, Bardram J, Tröster G. Pervasive healthcare: paving the way for a pervasive, user-centered and preventive healthcare model. Methods Inf Med 2010;49(1):67-73. [doi: 10.3414/ME09-02-0044] [Medline: 20011810]
4. Ruotsalainen PS, Blobel BG, Seppälä AV, Sorvari HO, Nykänen PA. A conceptual framework and principles for trusted pervasive health. J Med Internet Res 2012;14(2):e52 [FREE Full text] [doi: 10.2196/jmir.1972] [Medline: 22481297]
5. Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. ACM Comput. Surv 2012 Nov 01;45(1):1-54. [doi: 10.1145/2379776.2379779]
6. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 2012 Feb;36(1):93-101 [FREE Full text] [doi: 10.1007/s10916-010-9449-4] [Medline: 20703745]
7. Nykänen P, Seppälä A, Ruotsalainen P, Blobel B. Feasibility analysis of the privacy attributes of the personal wellness information model. Stud Health Technol Inform 2013;192:219-223. [Medline: 23920548]
8. Ruotsalainen PS, Blobel B, Seppälä A, Nykänen P. Trust Information-Based Privacy Architecture for Ubiquitous Health. J Med Internet Res 2013 Oct 08;1(2):e23. [doi: 10.2196/mhealth.2731]
9. Belanger F, Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly 2011;35(4):1017-1041.
10. Westin AF. Social and political dimensions of privacy. J Social Issues 2003 Jun;59(2):431-453. [doi: 10.1111/1540-4560.00072]
11. Lederer S, Deay AK, Mankoff J. A conceptual model and metaphor of everyday privacy in ubiquitous computing environments. UCB/CSD-2-1188, UC Berkeley College of Engineering Technical Reports. Berkeley, CA: Computer Science Division, University of California; 2002. URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2002/CSD-02-1188.pdf [accessed 2013-11-19] [WebCite Cache ID 1384860048852087]
12. Skinner G, Song H, Chang E. Defining and protecting meta privacy: a new conceptual framework within information privacy. 2006 Presented at: 22nd International Conference on Data Engineering Workshops; April 3-7, 2006; Atlanta, GA, USA. [doi: 10.1109/ICDEW.2006.46]
13. Smith JH, Dinev T, Xu H. Information privacy research - an interdisciplinary review. MIS Quarterly 2011;35(4):989-1016.
14. Clarke R. Internet privacy concerns confirm the case for intervention. Commun ACM 1999;42(2):60-67. [doi: 10.1145/293411.293475]
15. Pavlou PA. State of the information privacy literature: where are we now and where should we go? MIS Quarterly 2011;35(4):977-988.
16. Schoorman FD, Mayer RC, Davis JH. An integrative model of organizational trust: past, present, future. Academy of Management Review 2007 Apr 01;32(2):344-354. [doi: 10.5465/AMR.2007.24348410]
17. Abdul-Rahman A, Hailes S. A distributed trust model. In: New Security Paradigms Workshop: Proceedings, September 23-27, 1997, Langdale, Cumbria, United Kingdom. New York: Association for Computing Machinery; 1998.
18. Lu G, Lu J, Yao S, Yip J. A review on computational trust models for multi-agent systems. TOISCIJ 2009 Mar 19;2(2):18-25. [doi: 10.2174/1874947X00902020018]
19. Khiabani H, Sidek ZM, Manan JA. Towards a unified trust model in pervasive systems. In: 24th IEEE International Conference on Advanced Information Networking and Applications Workshops. Piscataway, NJ: The Institute of Electrical and Electronics Engineers, Inc; 2010 Presented at: Advanced Information Networking and Applications Workshops (WAINA), IEEE 24th International Conference on; 20-23 April 2010; Perth, WA p. 831-835. [doi: 10.1109/WAINA.2010.144]
20. Krukow K, Nielsen M, Sassone V. Trust models in ubiquitous computing. Philos Trans A Math Phys Eng Sci 2008 Oct 28;366(1881):3781-3793. [doi: 10.1098/rsta.2008.0134] [Medline: 18678555]
21. Joshi A, Finin T, Kagal L, Parker J, Patwardhan A. Security policies and trust in ubiquitous computing. Philos Trans A Math Phys Eng Sci 2008 Oct 28;366(1881):3769-3780. [doi: 10.1098/rsta.2008.0142] [Medline: 18672450]

22. Uddin GM, Zulkernine M, Ahamed SI. CAT: a context-aware trust model for open and dynamic systems. In: SAC '08 Proceedings of the 2008 ACM Symposium on Applied Computing. New York: ACM; 2008 Presented at: The ACM symposium on Applied computing; March 16-20, 2008; Brazil p. 2024-2029. [doi: 10.1145/1363686.1364176]
23. Schaub F, Koenings B, Dietzel S, Weber M, Kargl F. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, UbiComp 2012, CASEMANS 2012 Workshop. New York: ACM; 2012 Presented at: The ACM Conference on Ubiquitous Computing, UbiComp , CASEMANS Workshop; September 8, 2012; Pittsburgh, PA, USA p. 752-757. [doi: 10.1145/2370216.2370383]
24. Ruohomaa S, Kutvonen L. Trust management survey. Heidelberg: Springer; 2005 Presented at: Trust Management: Third International Conference, iTrust 2005; May 23-26, 2005; Paris, France p. 77-92. [doi: 10.1007/11429760_6]
25. Fitrianie S, Tatomir I, Rothkrantz L. A context aware and user tailored multimodal information generation in a multimodal HCI framework. : Eurosis; 2008 Presented at: EUROMEDIA; 2008; Ghent, Belgium p. 95-103.
26. Addas S. A call for engaging context in HCI/MIS-research with examples from the area of technology interruptions. AIS Transactions in Human-Computer Interaction 2010;2(4):178-196.
27. Johns G. In praise of context. J Organiz Behav 2001 Feb;22(1):31-42. [doi: 10.1002/job.80]
28. Dey AK, Abowd GD. Towards a better understanding of context and context-awareness.: GVU Technical Report; GIT-GVU-99-22; 1999. URL: https://smartech.gatech.edu/bitstream/handle/1853/3389/99-22.pdf [accessed 2014-03-06] [WebCite Cache ID 6Nrnzdg2F]
29. Dey A, Abowd G, Salber D. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. Human-Comp Interaction 2001 Dec 1;16(2):97-166. [doi: 10.1207/S15327051HCI16234_02]
30. Dourish P. What we talk about when we talk about context. Personal and Ubiquitous Computing 2004 Feb 1;8(1):19-30. [doi: 10.1007/s00779-003-0253-8]
31. Soylu A, Causmaecker P, Desmet P. Context and adaptivity in pervasive computing environments: links with software engineering and ontological engineering. Journal of Software 2009 Nov;4(9):992-1013. [doi: 10.4304/jsw.4.9.921-1013]
32. Viswanathan H, Chen B, Pompili D. Research challenges in computation, communication, and context awareness for ubiquitous healthcare. IEEE Commun. Mag 2012 May;50(5):92-99. [doi: 10.1109/MCOM.2012.6194388]
33. Paganelli F, Giuli D. An ontology-based system for context-aware and configurable services to support home-based continuous care. IEEE Trans Inf Technol Biomed 2011 Mar;15(2):324-333. [doi: 10.1109/TITB.2010.2091649] [Medline: 21075729]
34. Paganelli F, Giuli D. An ontology-based context model for home health monitoring and alerting in chronic patient care networks. : IEEE Computer Society Press; 2007 Presented at: 21st International Conference on Advanced Networking and Applications Workshops/Symposia; 21-23 May, 2007; Niagara Falls, Ontario, Canada p. 838-845. [doi: 10.1109/AINAW.2007.90]
35. Catarinucci L, Colella R, Esposito A, Tarricone L, Zappatore M. RFID sensor-tags feeding a context-aware rule-based healthcare monitoring system. J Med Syst 2012 Dec;36(6):3435-3449. [doi: 10.1007/s10916-011-9794-y] [Medline: 22083369]
36. Fenza G, Furno D, Loia V. Hybrid approach for context-aware service discovery in healthcare domain. Journal of Computer and System Sciences 2012 Jul;78(4):1232-1247. [doi: 10.1016/j.jcss.2011.10.011]
37. Das B, Seelye AM, Thomas BL, Cook DJ, Holder LB, Schmitter-Edgecombe M. Using smart phones for context-aware prompting in smart environments. 2012 Presented at: Consumer Communications and Networking Conference (CCNC), IEEE; 14-17 Jan. 2012; Las Vegas, NV p. 399-403. [doi: 10.1109/CCNC.2012.6181023]
38. Wongpatikaseree K, Ikeda M, Buranarach M, Supnithi T, Lim AO, Yasuo T. Activity recognition using context-aware infrastructure ontology in smart home domain. In: Proceedings 2012 Seventh International Conference on Knowledge, Information and Creativity Support Systems. Piscataway, NJ: The Institute of Electrical and Electronics Engineers, Inc; 2012 Presented at: Knowledge, Information and Creativity Support Systems (KICSS) Seventh International Conference; 8-10 Nov, 2012; Melbourne, VIC p. 50-57. [doi: 10.1109/KICSS.2012.26]
39. Zhang D, Yu Z, Chin CY. Context-aware infrastructure for personalized healthcare. Stud Health Technol Inform 2005;117:154-163. [Medline: 16282665]
40. Peleg M, Broens T, González-Ferrer A, Shalom E. Architecture for a ubiquitous context-aware clinical guidance system for patients and care providers. Heidelberg: Springer-Verlag; 2013 Presented at: KR4HC'13 / ProHealth'13; 2013; Murcia, Spain p. 161-167.
41. Jahnke JH, Bychkov Y, Dahlem D, Kawasame L. CEUR Workshop Proceedings (Vol. 114). 2004. Implicit, context-aware computing for health care URL: http://www.ics.uci.edu/~lopes/bspc04-documents/Jahnke.pdf [accessed 2013-11-19] [WebCite Cache ID 1384864716838609]
42. Bricon-Souf N, Newman CR. Context awareness in health care: a review. Int J Med Inform 2007 Jan;76(1):2-12. [doi: 10.1016/j.ijmedinf.2006.01.003] [Medline: 16488663]
43. Guarda P, Zannone N. Towards the development of privacy-aware systems. Information and Software Technology 2009 Feb;51(2):337-350. [doi: 10.1016/j.infsof.2008.04.004]
44. Pearson S, Casassa-Mont M. Sticky Policies: An Approach for Managing Privacy across Multiple Parties. Computer 2011 Sep;44(9):60-68. [doi: 10.1109/MC.2011.225]

45. Chakraborty S, Ray I. p-Trust: a new model of trust to allow finer control over privacy in peer-to-peer framework. JCP 2007 Apr 01;2(2). [doi: 10.4304/jcp.2.2.13-24]
46. Behrooz A, Devlic A. A context-aware privacy policy language for controlling access to context information of mobile users. In: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin Heidelberg: Springer; 2012:25-39.
47. Ghosh D, Joshi A, Finin T, Jagtap P. Privacy control in smart phones using semantically rich reasoning and context modeling. In: SPW 2012 IEEE CS Security and Privacy Workshops. Piscataway, NJ: The Institute of Electrical and Electronics Engineers, Inc; 2012 Presented at: Security and Privacy Workshops (SPW), IEEE Symposium; May 24-25, 2012; San Francisco, CA p. 82-85. [doi: 10.1109/SPW.2012.27]
48. Blount M, Davis J, Ebling M, Jerome W, Leiba B, Xuan L, et al. Privacy engine for context-aware enterprise application services. 2008 Presented at: Embedded and Ubiquitous Computing, EUC '08. IEEE/IFIP International Conference on , vol.2; 17-20 Dec. 2008; Shanghai p. 94-100. [doi: 10.1109/EUC.2008.130]
49. Carroll J. Five reasons for scenario-based design. Interacting with Computers 2000 Sep;13(1):43-60. [doi: 10.1016/S0953-5438(00)00023-0]
50. Rolland C, Ben Achour C, Cauvet C, Ralyté J, Sutcliffe A, Maiden N, et al. A proposal for a scenario classification framework. Requirements Eng 1998 Mar;3(1):23-47. [doi: 10.1007/BF02802919]
51. Nykänen P, Seppälä A. Collaborative approach for sustainable citizen-centered health care. In: Wickramasinghe N, Bali RK, Suomi R, Kirn S, editors. Critical Issues for the Development of Sustainable E-health Solutions (Healthcare Delivery in the Information Age). New York: Springer; 2012:115-134.
52. Seppälä A, Nykänen P, Ruotsalainen P. Development of personal wellness information model for pervasive healthcare. Journal of Computer Networks and Communications 2012;2012:1-10. [doi: 10.1155/2012/596749]
53. Seppälä A, Nykänen P. Contextual analysis and modeling of personal wellness. 2011 Presented at: the International Conference Knowledge Engineering and Ontology Development; Oct 2011; Paris, France p. 202-207.
54. Faravelon A, Chollet S, Verdier C, Front A. Enforcing privacy as access control in a pervasive context. 2012 Presented at: Consumer Communications and Networking Conference (CCNC) IEEE; 14-17 Jan; Las Vegas, NV p. 380-384. [doi: 10.1109/CCNC.2012.6181011]
55. Corradi A, Montanari R, Tibaldi D. Context-based access control management in ubiquitous environments. In: Network Computing and Applications. Los Alamitos, CA: IEEE Computer Society; 2004 Presented at: Third IEEE International Symposium on Network Computing and Applications; August 30-September 1, 2004; Cambridge, MA p. 253-260. [doi: 10.1109/NCA.2004.1347784]

Abbreviations

IT: information technology
PHS: personal health system

Edited by G Eysenbach; submitted 21.11.13; peer-reviewed by S Koch, J Zvarova, S Mohammed; comments to author 16.12.13; revised version received 26.01.14; accepted 12.02.14; published 11.03.14

Please cite as:
Seppälä A, Nykänen P, Ruotsalainen P
Privacy-Related Context Information for Ubiquitous Health
JMIR Mhealth Uhealth 2014;2(1):e12
URL: http://mhealth.jmir.org/2014/1/e12/
doi:10.2196/mhealth.3123
PMID: