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.

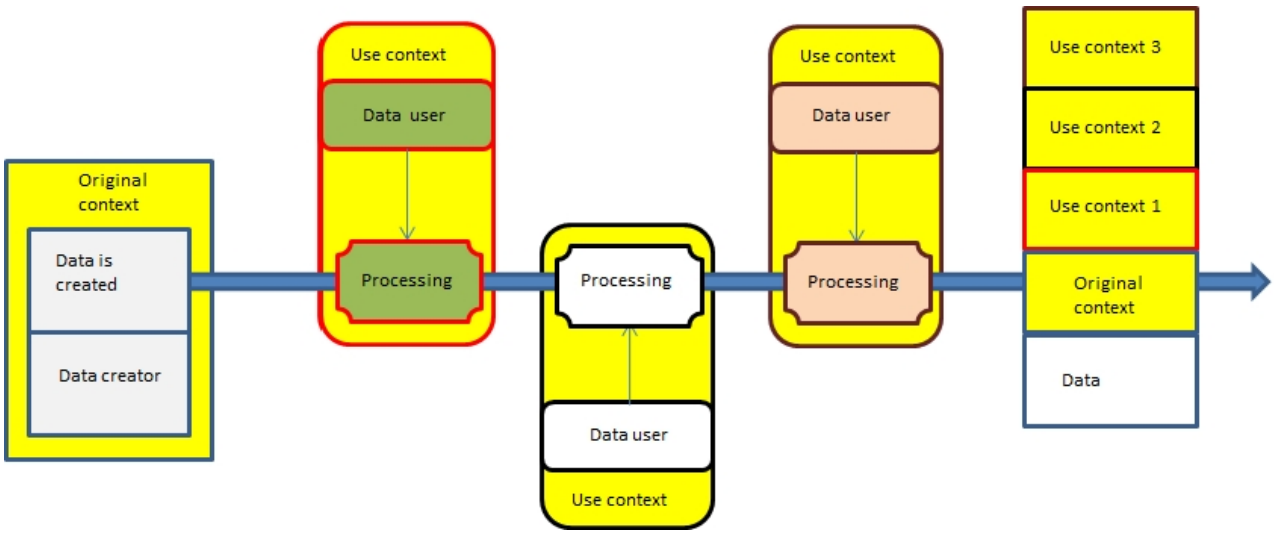
To protect his or her rights, an individual needs information about privacy, that is, privacy attributes, to define his or her personal privacy preferences. Privacy attributes enable privacy to be a concrete issue for individuals. In Nykänen et al [7], we defined privacy attributes as benefit, benevolence, 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.

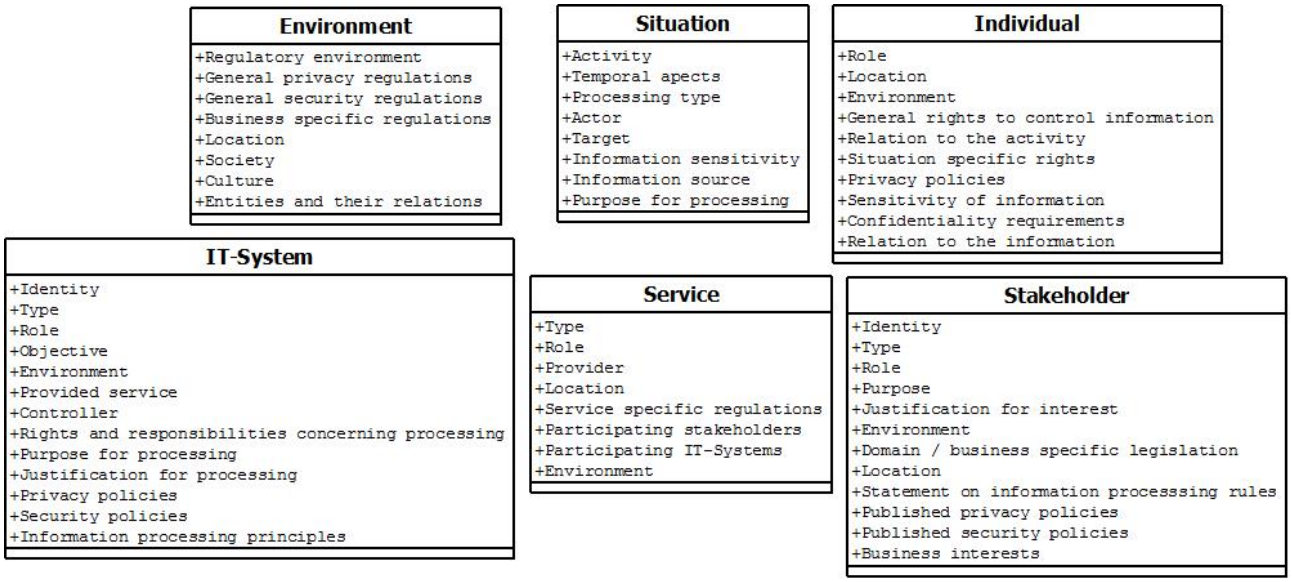
In a previous study [4], we defined ubiquitous health to be composed of services, information systems, stakeholders, and their environments. In addition to these, we have to capture the contexts of the information-processing situation and its object and/or subject. We should capture the following components 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.

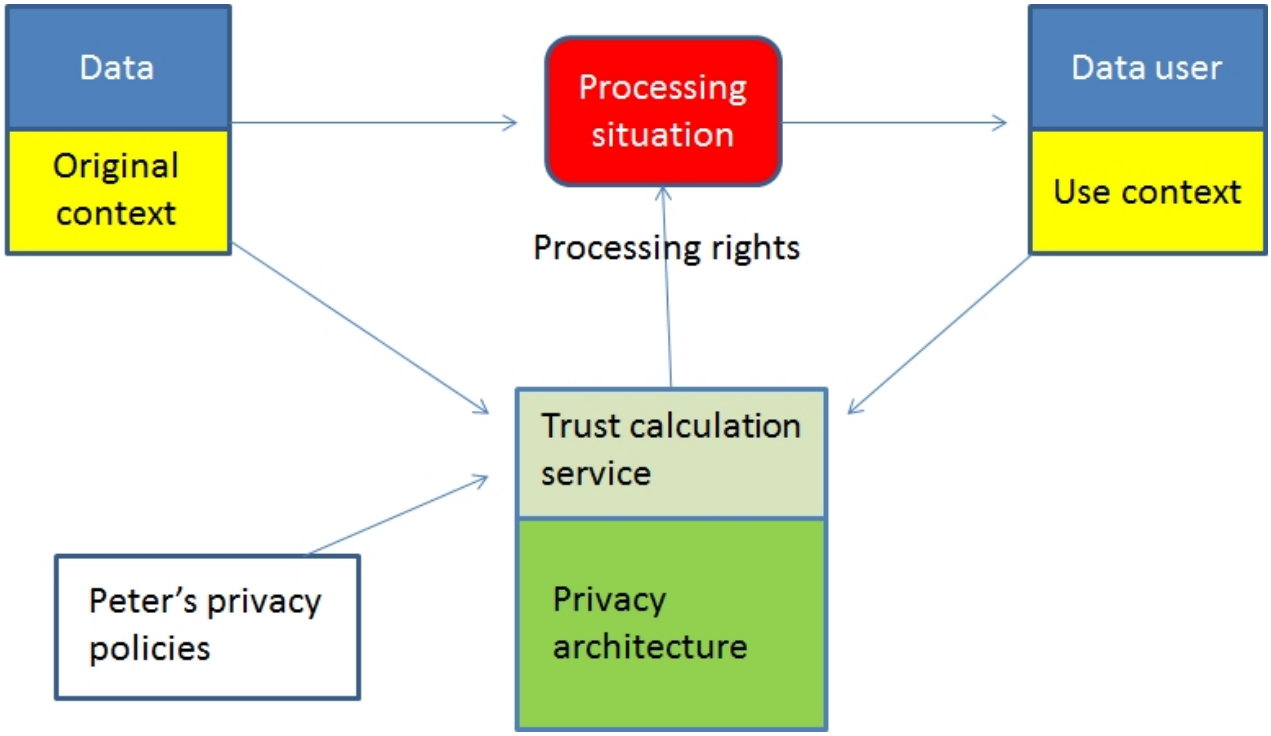
A service component describes regulated health care services and/or other services that can be offered by IT systems and/or stakeholders. An IT system component refers to all computational entities, which can include health information systems, personal health systems, ubiquitous systems, devices, sensors, 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

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 LJM. 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, Gonz alez-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 careURL: 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: 25100084