Privacy Issues in Pervasive Healthcare Monitoring System: A Review

Rusyaizila Ramli, Nasriah Zakaria, Putra Sumari

***Abstract*—**Privacy issues commonly discussed among researchers, practitioners, and end-users in pervasive healthcare. Pervasive healthcare systems are applications that can support patient's need anytime and anywhere. However, pervasive healthcare raises privacy concerns since it can lead to situations where patients may not be aware that their private information is being shared and becomes vulnerable to threat. We have systematically analyzed the privacy issues and present a summary in tabular form to show the relationship among the issues. The six issues identified are medical information misuse, prescription leakage, medical information eavesdropping, social implications for the patient, patient difficulties in managing privacy settings, and lack of support in designing privacy-sensitive applications. We narrow down the issues and chose to focus on the issue of 'lack of support in designing privacy-sensitive applications' by proposing a privacy-sensitive architecture specifically designed for pervasive healthcare monitoring systems.

***Keywords*—**Human Factors, Pervasive Healthcare, Privacy Issues

I. Introduction

UBIQUITOUS computing developments are growing rapidly as wireless technology becomes more reliable and able to support various types of applications. From ubiquitous computing is born another field, pervasive healthcare that combines ubiquitous computing and healthcare to develop applications that can assist patients in their daily life routines. Varshney [1] defines Pervasive Healthcare as "healthcare to anyone, anytime and anywhere by removing location, time and other restraints while increasing both the coverage and the quality of healthcare". This means, for instance, that a patient with heart problems can stay in the comfort of their own home while being monitored by healthcare services, instead of staying at the hospital.

On the other hand, there are many issues and challenges in realizing pervasive healthcare in daily life. These include the privacy aspect that has been identified based on the literature reviews conducted in this study. Most of the papers indicated that there is a need to address privacy in a pervasive healthcare system. Examples of Pervasive Healthcare applications include pervasive healthcare monitoring systems, intelligent emergency management systems, pervasive healthcare data access and ubiquitous mobile tele-medicine. However, this paper will focus on only pervasive healthcare monitoring systems since they pose more potential issues regarding patient privacy than other applications.

Privacy law generally defines an individual's privacy as personal information about an individual that can represent that individual as a whole, which consequently describes an individual. To protect their privacy, patients have the right to give permission as to which data should be collected, used or disclosed [2]. Without consent from the individual, his or her information should remain private; if any unauthorized person takes it, it is illegal action. As defined by Westin [3] privacy is "the claim of individuals, groups or institution to determine for themselves when, how and to what extent information about them is communicated to others".

Monitoring systems were chosen for this investigation because they deal more with data transactions, such as audio, video, or clinical data (blood pressure, heartbeat and electrocardiograph (ECG). "An electrocardiogram (ECG / EKG) is an electrical recording of the heart and is used in the investigation of heart disease" [4]. A monitoring system is a system that can monitor a patient daily without intruding on patient's daily routine. It could involve multiple parameters simultaneously; for example, the parameter could be reading the patient's ECG every few minutes or taking their blood pressure and sending it to their healthcare providers. A monitoring system could also involve, for example, transmitting live video and audio of a dementia patient to watch their behavioral to know her current condition. As it is pervasive, it means that most of the system components are wireless, therefore vulnerable to possible threats like eavesdropping and data theft; this raises privacy issues.

The next section discusses in detail the privacy issues in pervasive healthcare monitoring systems based on analysis of the research papers.

II. The Motivations

Please With the growing number of research and development projects in pervasive healthcare, many privacy issues and challenges arise; for that reason, we would like to understand the current issues and challenges. Patients have the

R. Ramli is with the School of Computer Sciences, Universiti Sains Malaysia, 11800 USM Penang, Penang, Malaysia (phone: (+604) 653 3888 ext 4392; fax (+604) 657 3335; e-mail: rusyaizila.cod08@student.usm.my).

N. Zakaria is with the School of Computer Sciences, Universiti Sains Malaysia, 11800 USM Penang, Penang, Malaysia (e-mail: nasriah@cs.usm.my).

P. Sumari is with the School of Computer Sciences, Univeristi Sains Malaysia, 11800 USM Penang, Penang, Malaysia (e-mail: putras@cs.usm.my).

right to choose whether or not to disclose their information and more individuals are becoming aware of privacy issues. Stronger security of a system would promise better privacy protection for the patients.

We selected published research papers that relate to ubiquitous computing, pervasive healthcare in general and pervasive healthcare monitoring systems. The criteria for selected papers are that they discuss security and privacy issues in the whole paper or at least in the introduction thus discussing the reasons behind the development of the system, architecture or model.

Figure 1 depicts the overview of the accumulated papers for the related topics. The graph shows that this topic was first discussed in 1993 by the founder of ubiquitous computing, Weiser [5]. Seven years later, Abowd and Mynatt [6] published a paper reviewing the past, present and future of ubiquitous computing. The paper gives an overview of what was discussed in the past and outlines the current situation in terms of technology and development in ubiquitous computing. In addition it includes suggestions for the future of ubiquitous computing, which is what the current developments now show.

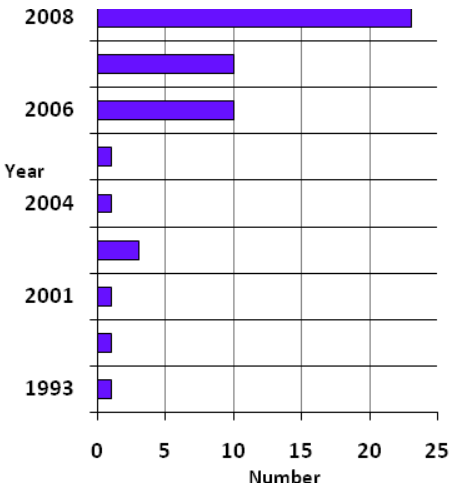

Fig. 1 Number of related published papers per year

In 2001, 2002, 2004 and 2005 respectively only one paper was published, while there are three published papers in 2003 regarding security and privacy issues and challenges in ubiquitous computing and pervasive healthcare. This shows the slow growth in research during this period. One of the reasons for the low publication rate is less interest by researchers in acknowledging privacy issues. During this period, the main research focus was technology development for ubiquitous computing and pervasive healthcare so as to make it exist in the world as envisioned by Wiser [5]. In 2006 and 2007 there are at least ten published research papers each year. The number of papers published related to these issues increased since 2006 compared to the years 2000 to 2005. In 2008, at least twenty-three papers were published discussing the security and privacy issues and pervasive healthcare development. This shows that the number of researchers that are interested in this field is increasing. Furthermore this shows that security and privacy issues are important to ensuring the success of pervasive healthcare development and implementation. In 2009, there were at least four papers published by the middle of May. The numbers are definitely going to increase and surpass what was produced in 2008, as these issues become more and more interesting due to the rapid development in pervasive healthcare systems.

Table 1 shows the summary of the seven selected scholar and research institutes that convey there are privacy issues is healthcare in general and how they would have suggested to overcome the issues.

TABLE I
SUMMARY OF SCHOLAR & RESEARCH INSTITUTES THAT CONVEY PRIVACY ISSUES

Study	Privacy Issues Concern	Conclusions
Weiser (1993) / Ubiquitous Computing	Ubiquitous computing touches many aspects in computer sciences including privacy	Privacy was a concern since the beginning of ubiquitous computing.
Abowd and Mynatt (2000) / Charting past, present, and future research in ubiquitous computing	Social implications of ubiquitous computing	There is no simple guideline to the direction of protecting privacy while applying ubiquitous computing in daily lives.
Kara (2001) /Protecting Privacy in Remote Patient Monitoring System	Someone may monitor the video transmission intentionally or accidentally.	Effective security can control privacy issues.
Schilit, Hong, Gruteser (2003) / Wireless Location Privacy Protection	Economic damages, location-based spam, harm to reputations	Suggested that researches have to find a solution to provide privacy as a component for the location based application [7]
Beckwith (2003) / Designing for ubiquity: The Perception of Privacy	Privacy and unawareness by patients and family member. Family rarely considered patient's privacy	Proposed works on interface that can auto remind patients to always updating their consent by time to time even they have agreed at the beginning of using the system. [8]
Varshney (2006) / Using Wireless Technology in Healthcare	Misuse of Patient Medical Information (MIS)	Works needed addressing privacy over wireless network where security still insufficient.
Wang et all (2008) / Pervasive and Trustworthy Healthcare	In medical information system (MIS), patients have major concern regarding security, privacy of the medical information.	Security and privacy of the MIS could be achieved by the combination of ubiquitous computing and security technologies in pervasive healthcare. [9]

The next section talks about the privacy issues in pervasive healthcare generally and in monitoring systems specifically. The issues discussed are based on the analyzed collected papers.

A. Healthcare Monitoring System

A healthcare monitoring system is a system that can monitor a patient's condition continuously to ensure help is sent immediately in case of emergency. The system can monitor a cancer patient's progress from home after treatment or it can monitor a schizophrenic patient's behavior at a psychiatric ward. A healthcare monitoring system can monitor various types of data and measurements depending on the patient's health problems.

A healthcare monitoring treatment system is a system that monitors the patient's treatment and evaluates their clinical state. This type of monitoring is important to ensure a patient's treatment is accurately recorded hence making it easier for healthcare professionals to provide follow up treatment. If the patient has a problem in future, all the stored data can be easily accessed to speed up the treatment decision. For example, there is an existing expert system for monitoring psychiatric treatment. The system is able to overcome the problem of monitoring drug treatment by assessing patient outcomes, employing a diagnostic checklist, and providing pharmacotherapy guidelines [10]. However, from the privacy perspective, storage of a patient's treatment data is vulnerable to data leakage or theft by information hackers and may lead to misuse of the patient's data.

Another type of patient monitoring is tracking a patient's physiological condition. One wireless physiological monitoring system for psychiatric patients has been developed by [11]. The system monitors two types of vital signs, oxygen saturation and heart rate, via electrocardiography (ECG) of a psychiatric patient wearing two types of devices. The signal is sent from the device to healthcare providers via Bluetooth connection. If any unusual vital signs are detected, help is immediately sent. The wireless connection could open more privacy issues as it has the potential security flaw of permitting unauthorized persons to steal the data hence intruding patient's privacy data. To protect the patient's privacy, the system should have strong privacy data management controls to lessen the privacy risk.

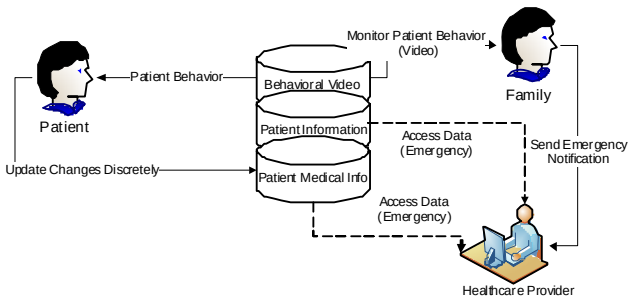

Fig. 2 Healthcare Monitoring System Overview

Fig.2 Depicts the general overview of a healthcare monitoring system used in this research. There are three main stakeholders that have privacy concerns in a healthcare monitoring system: the patient, the family and the healthcare providers. To illustrate how a healthcare monitoring system works, consider the following scenario. The patient is an elderly woman and the mother of a working daughter. The mother wants to live alone in the house; the daughter would like to be able to monitor the mother from her office. The monitoring system provides cameras in the house at a few possibly dangerous locations such as the kitchen and the living hall to monitor the patient's movement. The daughter can watch the video. The system is also connected to the mother's healthcare providers but they are not allowed to watch the video except in case of emergency. In order to protect the patient's data privacy, the healthcare provider also does not have any access to the patient's information unless there is an emergency. If there is an emergency with the patient, the daughter can send an emergency notification to the healthcare provider. Only then can the healthcare provider can retrieve all related patient information (such as name, address, medical history, prescription information, etc.) to send an ambulance and to provide adequate treatment. This type of restriction on monitoring of data can ensure the patient's privacy is protected and can decrease the possibility of data leakage.

III. Privacy Issues

Privacy issues derive from multidisciplinary fields such as computer science, bioinformatics, the social sciences and medical science. These days some pervasive healthcare applications are in development while patients have put other applications into use, therefore users and researchers are also starting to raise privacy issues. For example, before dementia patients agree to use the application, they and their relatives often ask about the privacy policies. This is because they want to ensure that their use either health is taken care of by the healthcare service providers while the privacy of their life is insured.

Based on the collected and analyzed privacy issues, we have summarized and grouped similar and related issues into six major privacy issues. The six issues identified are medical information misuse, prescription leakage, medical information eavesdropping, social implications for the patient, patient difficulties in managing privacy settings, and lack of support in designing privacy-sensitive applications. By doing this grouping, it would be easier for future research to know current issues in pervasive healthcare and embark upon the interested privacy issue.

A. Misuse of Patient Medical Information by Unauthorized Individual

In a pervasive healthcare monitoring system, patients are more exposed to privacy risks. A comprehensive monitoring system can be applied at the hospital, home or nursing home. The system can transmit signals from the patient to the healthcare provider when unusual signs are detected to get immediate help. When there is pervasive healthcare, the technology usually involves wireless communication; therefore it is open to all of the wireless threats such as eavesdropping and information theft. Thus one privacy issue would be the possible misuse of patient medical information by unauthorized personnel who can intercept and manipulate the information [12]. Without proper authentication and encryption unauthorized personnel can without any difficulty take patient data. Every pervasive system should incorporate basic encryption to protect the patient's information.

B. Prescription Leakage

Another issue that arises is the sale or transfer of prescription data from pharmacies or doctors to third parties [13]. Sale of detailed information about the patient that could portray a person completely is avoided because this is an obvious crime, therefore only part of the data can be sold. This raises the privacy issue of whether this can lead to the identification of a patient or not. In a pervasive monitoring system, patient data such as their prescriptions is saved in the database. This personal information is not sufficient to picture whom the exact person is; however if the third party is enthusiastic enough, they could combine the prescription information with other information that might be able on the net to eventually lead them to the exact patient. Finally they can go directly to the patient to promote drugs that might be suitable. The fascinating finding in this paper is that by only asking one colleague if he knew anyone who had been admitted to the hospital recently, and asking for general information such as gender, age and date admitted, the authors did some database searching and eventually found the details of the patient's drugs. What if this scenario happened to someone who was working with a pharmacy, for example? Without difficulty the third party can obtain a potential customer's information in order to sell their products. This is obviously violating patient's privacy.

C. Eavesdropping of Patient's Medical Information

A third potentially dangerous issue when applying monitoring technology is eavesdropping. Monitoring means that the system will record some patient data (such as blood pressure) to be transmitted to the healthcare providers. With these monitoring systems, it is easy for unscrupulous developers to make a system that can easily spy on the patient's data during the data transaction through wireless technology [6]. Therefore developers need to consider applying controlling authority whenever they develop a system. This can at least protect the patient's information from eavesdroppers or reduce the number of people that can easily take the information.

D. Social Implications for the Patients

Another privacy issue concerns the social implications for the patient. Some patients experience uneasiness or even fear while using the applications. It depends on the background of the patients like age, environment and life style. Some users would feel neglected being asked to use a computer system, others simply reject the technologies. This makes it even more difficult to ask them to use the system. For some users, they are curious to know what the application is doing – for example, in the case of a live monitoring application, users would like to know whether at that moment they are being recorded or not. They would then be able to control their private activity when they know that their movements are being watched. For this reason, a well-designed system should be able to tell the users the current recording status, such as the camera showing a green light when it is recording [6]. It is hoped that this can ensure patients feel confident enough to use the system. Besides that, users should have their own privacy control for the system, to block or to allow recording at specific times. However, this raises the question, 'what if something bad happens while the camera is turned off?' For this reason a system should be able to provide options to the users, such as turning off the monitor for a while with another backup emergency system.

Another implication to patient is when patient has some circumstances where he or she cannot decide owns privacy preferences. Therefore automatically the privacy preferences are authorized to the nearest family. For example older patient that might have dementia or psychiatric patient. Sometime family would have privacy concern for the patient however some family would find that privacy is not a matter to the patient prior to the health condition [14]. In sum, clearly defined privacy policies need to be developed that can help users to better optimize the privacy policy of the developed system.

E. Difficulties in Managing Privacy Policies

Users sometimes experience difficulties in managing privacy policy settings in a system. This is because of the limitations of devices and because sometimes users need to do various tasks at the same time. Users often feel it is difficult to set the privacy setting when they first begin using the application [15]. For example, if we are using a web chat application (i.e. Yahoo Messenger [16], MSN Messenger [17]) the first time we register we need to agree to the privacy setting before using the application. The agreement can be too long; hence users feel it is too much work to read and just accept the agreement. From time to time, the system will update the privacy settings, meaning that again users need to read and accept long sentences in the agreement text are always a burden for users to read, resulting in impracticality when users just accept the agreement. Therefore, the system needs to have practical, simple and easy privacy settings that can assist users in setting their privacy levels. In one paper [15] they developed three applications and did privacy testing, after which they evaluated the systems to see the impacts on user's privacy settings. This resulted in some interesting findings such as that a system has to be able to specify conservative default settings. This is to ensure that by default the system can conserve everything regardless of whether users notice or not. Later from time to time when users become aware of the privacy setting, they can alter privacy policies based on their preferences. For example, for the People Finder application, by default the system will make the user's location invisible to others. Later users can change the setting so certain people can know their locations. Another finding is that users seem to have difficulty defining their own policies. For that reason, researchers suggest that a system should have a learning dialogue and explanation technology to help users in defining their privacy policies [18]. Although researchers have suggested several findings to deal with listed issues, somehow they do not include the issue of privacy

setting for healthcare applications. For pervasive healthcare monitoring applications, the privacy policies setting would be a bit different as it opens more possible threat. The systems also need to have easy privacy management interfaces so that patients can set their policies. However, the system has to make sure that even though users can set the policies, yet the system has to have a boundary so all the crucial required data from the patient will be sent accordingly. A system cannot let the user specify settings that lead to misuse of a system so that the purpose of a system could not be fulfilled.

F. Lack of Support in Designing Privacy Sensitive Applications

Most of the above listed security and privacy issues are based on the user's perspective. From the developer's perspective, the issues would be a little bit different. Developers have little support in designing applications that are effective in helping users manage their privacy policies in applications [19]. Developers are eager to develop a pervasive healthcare monitoring system that applies the latest wireless technology and that can improve on previous applications. However, the privacy part of a system is somehow overlooked. Although developers have considered some privacy aspects, they only cover a narrow aspect of privacy; therefore developers tend to develop systems that fail to fulfill this user requirement. Because of this, users feel that the system is intrusive and end up refusing to use the system. As a result, Hong [19] has come out with Confab, a toolkit for facilitating the development of privacy sensitive applications. However, Confab is a toolkit for general application. We would like to develop a toolkit specifically targeted to pervasive healthcare monitoring applications that can assist developers in designing such applications. The resulting system could work better in assisting patients in managing their privacy policies and therefore provide a better healthcare application in future.

We have collected security and privacy issues in ubiquitous computing in general and in pervasive healthcare monitoring systems in particular that are focused on the human factors from the analysis of selected research papers [20-27] [9, 28-34]. Based on these issues, in the remainder of this paper we address privacy framework and propose a methodology for producing a privacy architecture that can be used by system developers to include a better design for privacy settings in their system requirements. Thus users, healthcare providers and developers can all benefit from the architecture. The next section will discuss the proposed work and the methodology in order to achieve the goal.

IV. Proposed Work

We have analyzed the privacy issues in ubiquitous computing in general and pervasive healthcare monitoring systems in particular in the previous section. In this section, we propose privacy architecture to enable the development of pervasive healthcare monitoring systems with a better privacy setting.

Even though previous work has been done to address these security and privacy issues, the works are generally on ubiquitous computing applications such as friend-finder applications and mobile tour guides [15, 19, 20, 26] few address pervasive healthcare privacy issues. In [35], the authors discuss possible security and privacy issues in pervasive healthcare monitoring systems focusing on data leakage. They mention that they want to address issues about patients' private information leakage by building a healthcare framework that will provide intelligent medical data acquisition. However, it does not mention how patients can manage their privacy settings on their own. Authors Hong and Landay [19] developed architecture for privacy sensitive ubiquitous computing applications in general to be used for applications such as friend finders. Our goal is to combine these two architectures to build a better privacy architecture that could be used by system developers to reduce data leakage and give users better control in managing their privacy policies.

The contribution of this research would be creating privacy sensitive architecture that can help behavioral psychiatric monitoring system ensuring patient's privacy. This research is going to be interesting, as psychiatric patients would have different privacy perspective and different concerns compared to other patients. Different type of psychiatric issues would define different level of disclosure. Furthermore their family has authority to define patient's privacy on behalf of them. Therefore we are going to analyze their privacy preferences based on their needs to help them protecting their privacy.

Figure 3 depicts the proposed framework for a privacy sensitive behavioral monitoring system. There are four stakeholders in this system: patient, family, application developer and healthcare provider. Patient and family will be informed of their privacy policy first as a guideline, before they define their privacy management.

Patient and family defined as end users in the system as they have authority to define their privacy preferences through the user interface. Their privacy setting will go through End-Users Privacy Management Module. The privacy preferences will be combined with privacy management in the system, which contains privacy policies that are collected during the initial phase of this research. The combination of these two privacy managements will define the multiple data storage in this system. in other words, users automatically have control on their privacy such as who can view their video and how long the data could be saved on the database. The application developer's role is to develop a monitoring system that has a privacy architecture that will guarantee the system will work well with patient's privacy preferences. The healthcare provider has access to vital signs data and certain additional data as permitted by patients and family.

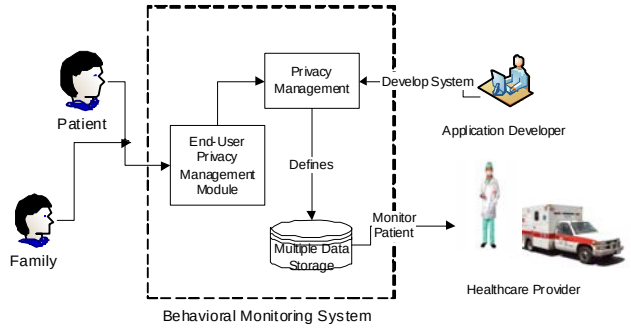

Fig. 3 Proposed Framework for Privacy-Sensitive Monitoring System

To achieve the goal of this work, we are going to gather privacy policy requirements by doing document analysis. The document analysis would specify type of hospital polices, obtain related documents on privacy, interview few experts and as for the outcome is the comprehensive privacy guidelines. After the first phase, we proceed by developing privacy management module. This is going to be the gathering of user requirements through survey and interview that involve the stakeholders mentioned in previous section. Next phase is the design of privacy module prototype to check the interface design and develop the privacy management module and evaluate the design. We will then later evaluate the design then finally implement the design.

V. Conclusions

In this paper, we have discussed the privacy issues in ubiquitous computing in general and in pervasive healthcare monitoring systems in particular, based on an analysis of collected research papers. Each of the issues listed have been discussed in detail and we have proposed suggestions to address each of them. From the issues, we chose one to be addressed in our subsequent research that is the privacy policy management difficulties faced by end users of a pervasive healthcare monitoring system. To address these difficulties, we plan to propose architecture for a privacy-sensitive pervasive monitoring system. The requirements will be gathered from end users and application developers. The architecture will provide a framework that can be used by application developers to develop a privacy-sensitive application for the end users.

References

[1] Varshney, U.: Pervasive healthcare and wireless health monitoring. Mob.Netw. Appl. 12 (2007) 113-127
[2] Kosseim, P., Emam, K.E.: Privacy Interests in Prescription Data, Part I: Prescriber Privacy. IEEE Security and Privacy 7 (2009) 72-76
[3] Westin, A.F.: Privacy and Freedom. The Bodley Head Ltd (1970)
[4] Jenkins, D., Gerred, S.: Electrocardiogram (ECG, RKG) library. Vol. 2009
[5] Weiser, M.: Hot topics-ubiquitous computing. Computer 26 (1993) 71-72
[6] Abowd, G.D., Mynatt, E.D.: Charting past, present, and future research in ubiquitous computing. ACM Trans. Comput.-Hum. Interact. 7 (2000) 29-58
[7] Schilit, B., Hong, J., Gruteser, M.: Wireless Location Privacy Protection. Computer 36 (2003) 135-137
[8] Beckwith, R.: Designing for Ubiquity: The Perception of Privacy. IEEE Pervasive Computing 2 (2003) 40-46
[9] Kai, W., Yan, S., Xukai, Z., Durresi, A., Shiaofen, F.: Pervasive andTrustworthy Healthcare. Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference (2008) 750-755
[10] Goethe, J.W., Bronzino, J.D.: An expert system for monitoring psychiatric treatment. Engineering in Medicine and Biology Magazine, IEEE 14 (1995) 776-780
[11] A.J, R.: Wireless physiological monitoring for psychiatric patients. Mechanical and Mechatronic Engineering, Vol. MScEng. University of Stellenbosch (2008)
[12] Varshney, U.: Managing Comprehensive Wireless Patient Monitoring Pervasive Health Conference and Workshops, 2006 (2006) 1-4
[13] Dai, P.-D., Zhang, T.-Y., Wang, Z.-M., Chen, J.X., Wang, K.-Q.: Privacy Interests in Prescription Data, Part 2: Patient Privacy. Computing in Science and Engg. 7 (2009) 75-78
[14] Adams, A., Martina, M., Sasse, A., Sasse, M.A.: Privacy in Multimedia Communications: Protecting Users, Not Just Data. Springer (2001) 49-64
[15] Cornwell, J., Fette, I., Hsieh, G., Prabaker, M., Rao, J., Tang, K., Vaniea, K., Bauer, L.Cranor, L., Hong, J., McLaren, B., Reiter, M., Sadeh, N.: User-Controllable Security and Privacy for Pervasive Computing. 8th IEEE Workshop on Mobile Computing Systems and Applications (HotMobile 2007), Vol. 8 (2007)
[16] Yahoo Web Messenger, http://messenger.yahoo.com
[17] Microsoft: Windows Live Messenger, http://mail.live.com/mail/MSNWebIMDecomm.aspx
[18] Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., Rao, J.: Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application. Journal of Personal and Ubiquitous Computing (2008) 14
[19] Hong, J.I., Landay, J.A.: An architecture for privacy-sensitive ubiquitous computing. Proceedings of the 2nd international conference on Mobile systems, applications, and services. ACM, Boston, MA, USA (2004)
[20] Hong, J., Satyanarayanan, M., Cybenko, G.: Security & Privacy. Pervasive Computing, IEEE (2007)
[21] Kara, A.: Protecting Privacy in Remote-Patient Monitoring. Computer 34 (2001) 24-27
[22] Kelley, P.G., Drielsma, P.H., Sadeh, N., Cranor, L.F.: User-Controllable Learning of Security and Privacy Policies. ACM CCS 2008 Conference (2008)
[23] Kim, J., Beresford, A., Stajano, F.: Towards a Security Policy for Ubiquitous Healthcare Systems (Position Paper). Ubiquitous Convergence Technology (2007) 263-272
[24] Martino, L.D., Qun, N., Dan, L., Bertino, E.: Multi-domain and privacy-aware role based access control in eHealth. Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference (2008) 131-134
[25] Puzar, M., Plagemann, T., Roudier, Y.: Security and privacy issues in middleware for emergency and rescue applications. Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference (2008) 89-92
[26] Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., Rao, J.: Understanding and capturing people's privacy policies in a mobile social networking application. Personal Ubiquitous Comput. 13 (2009) 401-412
[27] Weerasinghe, D., Elmufti, K., Rajarajan, M., Rakocevic, V.: Patient's privacy protection with anonymous access to medical services. Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. (2008)127-130
[28] Adlam, T.D., Evans, N., Gibbs, C., Orpwood, R.: User Evaluation of Smart Flats for People with Dementia. Pervasive Health Conference and Workshops, 2006 (2006) 1-4
[29] Butz, A., Kruger, A.: User-centered development of a pervasive healthcare application. Pervasive Health Conference and Workshops (2006) 1-8
[30] Dong, C., Dulay, N.: Privacy Preserving Trust Negotiation for Pervasive Healthcare. Pervasive Health Conference and Workshops, 2006 (2006) 1-9

[31] Elmufti, K., Weerasinghe, D., Rajarajan, M., Rakocevic, V., Khan, S.: Privacy in Mobile Web Services eHealth. Pervasive Health Conference and Workshops, 2006 (2006) 1-6
[32] Jacobsson, M., Niemegeers, I.: Privacy and anonymity in personal networks. Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on (2005) 130-135
[33] Jae Hun, L., Jin Kyu, P., Sang Wook, K.: User-Directed Privacy Protection in the Ubiquitous Environment. Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on, Vol. 2 (2008) 37-42
[34] Jasemian, Y.: Security and privacy in a wireless remote medical system for home healthcare purpose. Pervasive Health Conference and Workshops, 2006 (2006) 1-7
[35] Ahamed, S.I., Talukder, N., Kameas, A.D.: Towards privacy protection in pervasive healthcare. Intelligent Environments, 2007. IE 07. 3rd IET International Conference on (2007) 296-303