Managing Disclosure of Personal Health Information in Smart Home Healthcare

Umar Rashid, Hedda Schmidtke, and Woontack Woo

U-VR Lab, GIST
{urashid, schmidtk, wwoo}@gist.ac.kr

Abstract. Recent advances in ubiquitous computing have evoked the prospect of real-time monitoring of people's health in context-aware homes. Home is the most private place for people and health information is of highly intimate nature. Therefore, *users-at-home* must have means to benefit from home healthcare and preserve privacy as well. However, most smart home healthcare systems currently lack support for privacy management for home inhabitants. In this paper, we analyze the privacy needs of smart home inhabitants utilizing a healthcare system and present a conceptual framework to manage disclosure of their personal health information. The proposed framework supports sharing the most meaningful detail of personal health information at different time granularities with different recipients in different contexts. To relieve the burden of configuration, default disclosure settings are provided, and to ensure end-user's control over disclosure, the option to override default settings is included.

Keywords: Information disclosure, privacy, context awareness, home healthcare.

1 Introduction

The emerging advances in pervasive computing technologies hold great potential for improving people's quality of life. One of the most promising area of applications of these technologies is home healthcare [6, 15, 22]. In recent years, remote monitoring of patients in real-time via wearable health monitoring devices has become a special focus of interest [25]. Its promises notwithstanding, many researchers have expressed concerns about the potential privacy breaches associated with real-time health monitoring in home environment. Home remains the safest and the most private place for people [21] and health information is of highly sensitive nature as it can reveal intimate aspects about a person's life [11, 32]. Therefore, it is crucial to guarantee the respect of personal privacy in smart home healthcare [4, 22].

To date, most smart home health projects [6,15,22] have overlooked the privacy management for *users-at-home* in their design. We also found the current literature deficient in detail about guidelines how to incorporate privacy support in the design of smart home healthcare systems. To avail the promised benefits of home healthcare, smart home inhabitants should be able not only to prevent unwanted disclosure of

C. Stephanidis (Ed.): Universal Access in HCI, Part II, HCII 2007, LNCS 4555, pp. 188–197, 2007.

personal health information but moreover, to share the *most meaningful* details of information with different recipients in different contexts. In healthcare domain, trust refers to the competence as well as beneficence of the trustee [5]. We found most privacy models for ubiquitous computing systems [1, 9, 13, 17] insufficient for our purpose because they do not explicitly incorporate the competence of information recipients as a determinant for information disclosure.

In this paper, we first analyze the privacy requirements for end-users of smart home healthcare. Our analysis draws on studies in the domains of ubiquitous computing, and health information management, and on sociological readings on interpersonal relationships. Based on the requirement analysis, we construct a theoretical framework that helps the end-users manage the disclosure of personal health information in different contexts. The proposed framework is founded upon 5W1H (Who, Where, When, What, How and Why) context model proposed by Jang et al. [14]. In our application scenario, personal health information consists of raw physiological data that is collected via wearable sensors and processed stress level that is result of analysis of collected physiological data based on Oriental Medical Science [10]. To extract the most meaningful details about personal health information in emergency as well as normal situations, we classify the information at different time granularities using a variant of a clustering algorithm specified in [30]. To relieve the end-user of the burden of configuration, we provide default disclosure settings in changing contexts. However, to ensure that the end-user remains in control over the disclosure of his/her personal health information, we also include the option to override default settings.

The paper is organized as follows. In the section 2, we provide a requirement analysis for end-user's privacy in smart home healthcare. The conceptual framework to tackle privacy management in smart home healthcare is explained in section 3. Section 4 deals with an experimental demo illustrating our framework. We wrap up with a summary of current work and directions for future works in the section 5.

2 Privacy Requirements for Users of Smart Home Healthcare

Due to recent advances in ubicomp technologies, home healthcare is expected to become a usable means of health provision in the not so distant future. The concept of "smart home healthcare" deals with the use of sensors and actuators in home environment for real-time monitoring of occupants' health status. Many laboratories and companies are currently working on research projects in this field. Among these, some of the most prominent include the "Aware Home" at Georgia Institute of Technology [15], the "Center for Future Healthcare" at University of Rochester [6], and the "Intelligent Habitat for Health" at Faculty of Medicine of Grenoble [22]. However, to date, research in this domain has paid little attention to information systems and decision support for patients [16]. In particular, patients' perspective on privacy management in real-time health monitoring [4] remains under-explored in literature.

One of the prime challenges in personal health information management (PHIM) is "sharing information with individuals from social, professional, and health-care networks while maintaining personal privacy" [28]. Studies have emphasized the need for individuals' control over personal health information [31]. Surveys highlight the fact that many people consider their health information to be highly confidential [32], second only to financial information [11]. The 1993 Harris Equifax Health Information Privacy Survey found that 25% of the public scored high in general privacy concern, however, when measured specifically for medical privacy concern, 48% fell into the high concern position [12].

Use of wearable computing devices for real-time monitoring of health poses serious privacy issues for patients [20]. Real-time surveillance of personal health in home environment makes an individual's ability to preserve privacy more tenuous [4]. The classified nature of both the health information and the home signify the pressing importance of privacy management for users of smart home healthcare [21, 22]. An ethnographic study of a community living with ubiquitous computing [3] points out that:

- Users do not understand the possibilities and implications of privacy breaches in residential care.
- Users often forget that they are being monitored.
- Users trust the designers of a system to have protected them from unanticipated consequences.

The aforementioned findings indicate the gravity of the task before the system designers to offset potential privacy violations associated with home healthcare in ubiquitous computing environments. As stated by Adams and Sasse [1], "Most invasions of privacy are not intentional but due to designers' inability to anticipate how this data could be used, by whom, and how this may affect users". It is desirable to provide default privacy settings in the system to relieve the user of the burden of configuration [27]. It has also been noticed that most users are unlikely to change the default settings [27]. On the other hand, it is also important to empower people "to stipulate what information they project and who can get hold of it" [7]. Hence, the option to override default settings must be provided as well.

People's willingness to share information is likely to differ depending upon the kind of information and who is likely to view it [23]. Instead of a coarse-grained approach of denying/allowing access to personal information, ubiquitous computing systems must allow for granular control to fine-tune the details of disclosed information [13]. Patel et al. [26] discovered that most users rate family more trustworthy than the friends and colleagues. Chatfield et al [7] conducted a study to examine user's opinions on personal information exchange with an Intelligent Environment. They discovered that the biggest influence on a user's information sharing preferences was the existence of a prior relationship with the information recipient. In other words, the parameter of s*ocial intimacy* is a determining factor in information sharing.

In the context of healthcare, trust refers to the "confidence in competence (skill and knowledge), as well as whether the trustee is working in the best interests of the trustor" [5]. People show high degree of trust in physicians to access their medical records while an overwhelming majority opposes their records to be shown to employers [11]. Confidentiality in patient-doctor relationship even outranks that in patient-family relationship [2]. Patients have high level of trust for their family physicians that gives them comfort to reveal personal and sensitive information [19, 31]. Patients reveal even those details about personal health to their doctors which they feel hesitant to share with their families. Moreover, many family members, because of low health literacy, may be unable to understand arcane technical details of health information. This suggests that in the matters of healthcare, people's willingness to share information is not only motivated by *social intimacy* to the recipient but also by the *competence* of the recipient.

Palen and Dourish [24] describe privacy management as a "dynamic response to circumstance rather than a static enforcement of rules". Lederer et al. found out that in ubiquitous computing, the recipient's identity is a stronger determinant of privacy preferences than the user's situation [18]. However, in ubicomp healthcare, users are likely to prefer privacy settings for normal situations to be set aside under emergency situations [13]. In an emergency, safety takes precedence over privacy, and most patients will probably choose a "confidentiality override policy" that would allow an authenticated healthcare provider to gain access to records that he/she would normally not be entitled to view [19]. Hence, disclosure settings of health information in smart home healthcare must make room for adapting to the changes in the user's situation.

Based upon the abovementioned observations, we specify the criteria to assess what constitutes *the most useful* information to be disclosed to a particular recipient under a particular situation in smart home healthcare. Our conclusion is that such decision is determined by the following factors:

- Social intimacy between the end-user and the recipient
- Competence of the recipient
- Situation of the end-user

3 Personal Health Information Disclosure Management

Based on the analysis of privacy needs of end-users of smart home healthcare, we present a conceptual framework that helps them manage disclosure of personal information. We use the user-centric context model of Jang et al [14] to represent the constituents of our proposed framework. According to this context model, context information is organized using the categories of involved users ('Who'), spatial circumstance ('Where'), time ('When'), involved objects, pieces of information, and services ('What'), current state ('How'), and further information on causes for user interaction ('Why'). The following components of 5W1H (Who, Where, When, What, How and Why) context model [14] are utilized for Personal Health Information Disclosure Management (PHIDM) framework:

- Personal Health Information ('What')
- Situation of the end-user represented by his/her stress level in one-minute-interval ('How')
- Competence of the information recipient ('Who')
- Intimacy between the information recipient and the end-user ('Who')

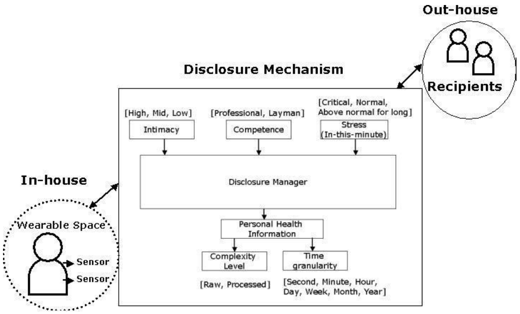


Fig. 1. Framework for Personal Health Information Disclosure Management (PHIDM)

The inputs and outputs of the disclosure mechanism are illustrated in Fig. 1. Personal health information is classified into two categories with respect to its complexity level i.e.

- Raw - physiological data ('Expert' information)
- Processed - stress level data ('Layperson' information)

Raw data consists of galvanic skin response, pulse rate, and temperature of the patient collected via wearable sensors. Processed information (stress level) is obtained by interpreting this raw data on the basis of Oriental Medical Science analysis [10].

Taking cue from Rogers et al [29], the granularity of disclosed information is set to day (24 hours) level, under normal situations. To provide a more in-depth view of the end-user's situation at different temporal granularities (second, minute, hour, day, week, month, year), we apply a variant of clustering mechanism derived from the specification provided in [30]. This corresponds to '*details-on-demand*' functionality proposed by Chittaro [8] that allows for visualization of patient's medical record at different temporal granularities on mobile devices.

Situation of the end-user is represented by the level of his/her stress during one-minute-level intervals as follows:

- Normal
- Above-normal over long duration
- Critical

Competence refers to the recipient's skills and knowledge to comprehend health information, and is categorized as:

- Professional (healthcare professionals)
- Layperson (non-healthcare people)

Based on the studies about interpersonal relations [2, 18, 23, 26] and health information privacy [11, 19, 31], we specify three levels of intimacy between the recipient and the end-user as given below:

- High (family physician, significant others, close family members)
- Medium (emergency healthcare staff, close friends)
- Low (colleagues, employers, acquaintances that need to be informed in critical situations)

Under normal situation, access to personal health information is provided *on demand* only, however, in other situations, the recipients are *notified* and provided information according to the default settings. If not overridden by the end-user, the default disclosure settings operate as follows:

If the user's stress level is critical

- Notify the High, Medium and Low intimacy contacts
- Set time granularity of disclosed information to one-minute-interval
- Set complexity of information with respect to competence of the recipient

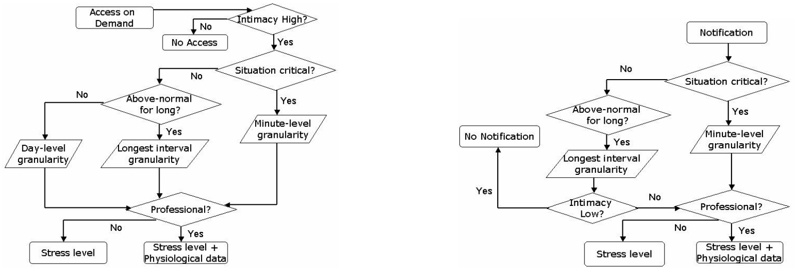
Else if the user's stress level is above-normal for long duration

- Notify High and Medium intimacy contacts
- Set time granularity of disclosed information to the largest interval of above-normal stress (hour, day, week, month, year)
- Set complexity of information with respect to competence of the recipient

Else if the user's stress level is normal

- Allow access for information only to High intimacy contacts
- Set time granularity of disclosed information to day
- Set complexity of information with respect to competence of the recipient

The illustration of disclosure management algorithm under the modes of '*access on demand*' and '*notification*' are shown in Figs. 2.a and 2.b respectively.



(a) (b)

Fig. 2. Illustration of disclosure management algorithm (a). Access on Demand (b). Notification.

The physiological data of a patient (e.g. pulse rate, galvanic skin response) can be *meaningful information* to be shared with doctors. However, this information remains arcane to family members and coworkers (because of their low health literacy). Hence, it is *meaningful* to let them know about interpreted stress condition only. Similarly, it is reasonable to share stress information with employers and coworkers in an emergency. But otherwise, it is not desirable to let them access personal health information. Moreover, in an emergency situation, it is *most meaningful* for the user to disclose up-to-date, fine-grained information about stress condition, therefore, setting granularity to "minute" level. In normal situation, coarse-grained information about long-term trends of user's stress condition becomes *most meaningful*, hence, setting the granularity to "Day" level.

4 Experimental Demo

In our experimental demo, physiological data of end-users is collected from a wearable wrist type sensor system including a PPG sensor, a GSR sensor and an SKT sensor, as shown in Fig. 3. Collected data is sent to an Ultra-Mobile Personal Computer (UMPC) via blue tooth connection and interpreted into stress level on the basis of Oriental Medical Science analysis [10]. Interface to specify intimacy levels and user-specified settings (i.e. overrule the default settings) are provided on the end-user's UMPC as shown in Fig. 4. Competence of the recipients is determined by their profiles stored on their respective UMPCs.

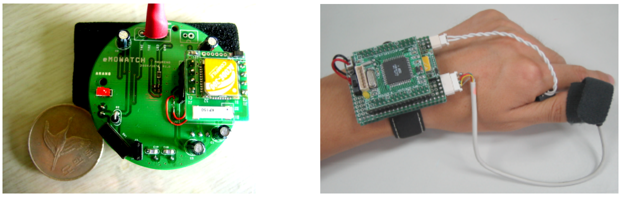
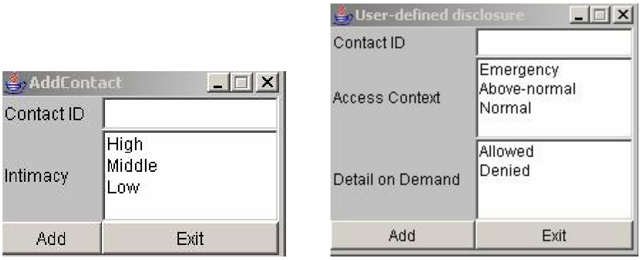


Fig. 3. Wearable sensor system


AddContact

Contact ID

Intimacy: High, Middle, Low

User-defined disclosure

Contact ID

Access Context: Emergency, Above-normal, Normal

Detail on Demand: Allowed, Denied

(a) (b)

Fig. 4. End-user's interface to (a) specify intimacy level of recipients (b) user-specified disclosure settings (i.e. overrule default settings)

Figure 4 shows the stress information being shown on the device of personal physician and Fig. 5 illustrates the stress information to be displayed on the device of family members (competence: 'layman' level). Figure 6 shows the data to be displayed on the devices of emergency healthcare staff under emergency situation.

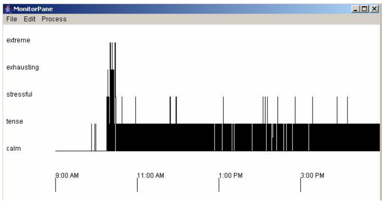


Fig. 5. Data accessible to personal physician

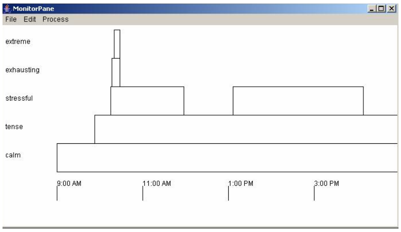


Fig. 6. Data accessible to family members (Competence level: layman)

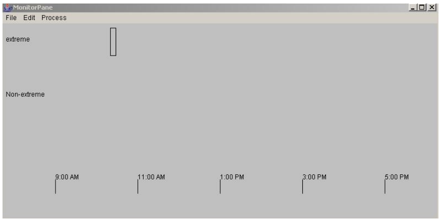


Fig. 7. Data accessible to emergency healthcare staff and employers etc. (Intimacy level: Middle or Low)

5 Conclusions and Future Works

In this paper, we analyzed the privacy requirements for end-users of smart home healthcare and presented a conceptual framework for managing disclosure of personal health information. The primary aim of the proposed framework is not to prevent disclosure of user's health information but to share the most meaningful detail with different recipients in different contexts. It allows for fine-grained control over disclosure of health information, adapts disclosure rules with respect to end-user's context, and provides default disclosure settings to relieve end-users of the burden of configuration. The framework also includes the option to override the default disclosure rules for specific recipients and specific situations.

In future works, we intend to broaden the mechanism of personal information disclosure management from smart home to a ubiquitous smart space. In that scenario, the scope of personal information is not limited to health information but also encompass e.g. location information. This will call for taking spatial granularity into account, in addition to time granularity, in order to determine what is the *most meaningful* personal information in different contexts.

Acknowledgments. This work was supported by Seondo project, Ministry of Information and Communication, Republic of Korea.

References

1. Adams, A., Sasse, A.: Privacy in Multimedia communications: Protecting users, not just data. In: Joint Proc. Human-Computer Interaction/Interaction d'Homme-Machine (IMH-HCI 01), pp. 49–64. Springer, Heidelberg (2001)
2. BBC Health - Talking to your doctor - Patient confidentiality http://www.bbc.co.uk/health/talking_to_your_doctor/gp_confidentialitypatient.shtml
3. Beckwith, R., Lederer, S.: Designing for One's Dotage: Ubicomp and Residential Care Facilities. In: Proc. HOIT 2003, Center for Research on Information Technology and Organizations (2003)
4. Blanchard, J.: Ethical considerations of Home Monitoring Technology. Home. Health Care. Technology Report 53(4), 63–64 (2004)
5. Calnan, M., Row, R.: Trust Relations in the new NHS: theoretical and methodological challenges. Taking Stock of Trust E.S.R.C Conference, LSE (2005)
6. Center for Future Healtth http://www.futurehealth.rochester.edu/
7. Chatfield, C., Häkkilä, J.: Designing Intelligent Environments - User Perceptions on Information Sharing. In: Proceedings of the Asia-Pacific Conference on Computer and Human Interactions, pp. 570–574 (2004)
8. Chittaro, L.: Visualization of Patient Data at. Different Temporal Granularities on Mobile Devices. In: Proc. of AVI, pp. 484–487 (2006)
9. Mather, B.V., Sellen, A.: Design for privacy in ubiquitous computing environments. In: Proc. ECSCW (1993)
10. Choi, A., Rashid, U., Woontack, W.: Context-based user adaptive physiological signal analysis. In: Proc. KHCI, pp. 960–965 (2006)
11. Gallup Organization. Public attitudes towards privacy (2000)
12. Harris-Equifax.: Consumer privacy survey, conducted for Equifax by Louis Harris and Associates in association with Dr Alan Westin of Columbia University.Atlanta, GA: Equifax (1996)
13. Hong, J.I., Landay, J.A.: An architecture for privacy-sensitive ubiquitous computing. In: Proc. MobiSys 2004, pp. 177–189. ACM Press, New York (2004)
14. Jang, S., Woo, W.: Unified Context Representing User-Centric Context: Who, Where, When, What, How and Why. ubiComp workshop (ubiPCMM), pp. 26–34 (2005)
15. Kidd, C.D., Orr, R.J, Abowd, G.D., Atkesson, C.G., Essa, I.A., MacIntyre, B., Mynatt, E., Starner, T.E., Newsletter, W.: The aware Home: A living Laboratory for ubiquitous computing research. In: Proc. CoBuild'99 (October 1999)
16. Koch, S.: Home Telehealth - current state and future trends. Elsevier International Journal of Medical Informatics (2005)
17. Lederer, S., Mankoff, J., Dey, A., Beckman, C.: Managing Personal Information Disclosure in Ubiquitous Computing Environments. Technical Report IRB-TR-03-015, Intel Research Berkley (2003)
18. Lederer, S., Mankoff, J., Dey, A.: Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. Extended Abstracts of CHI, pp. 724–725 (2003)

19. Mandl, K.D., Szolovits, P., Kohane, I.S., Markwell, D., MacDonald, R.: Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ 322 7281, 283–287 (2001)
20. Martin, T., Jovanov, E., Raskovic, D.: Issues in Wearable Computing for Medical Monitoring Applications: A Case Study of a Wearable ECG Monitoring Device. In: Proc. 4th Int. Symposium on Wearable Computers, pp. 43–49 (2000)
21. Meyer, S., Rakotonirainy, A.: A Survey of Research On Context-aware Homes. In: Proc. Australasian Information Security Workshop Conference on ACWS Frontiers, pp. 159–168 (2003)
22. Noury, N., Virone, G., Barralon, P., Rialle, V., Demongeot J.: New trends in health smart homes: technological possibilities, societal concerns, economical constraints. In: IEEE Transactions on Information Technology in Biomedicine (TITB-119-2003)
23. Olson, J.S., Grudin, J., Horvitz, E.: A study of preferences for sharing and privacy. In: Extended Abstracts CHI2005, pp. 1985–1988. ACM Press, New York (2005)
24. Palen, L., Dourish, P.: Unpacking Privacy for a Networked World. In: Proc. CHI 2003, pp. 129–136. ACM Press, New York (2003)
25. Park, S., Jayaraman, S.: Enhancing the quality of life through wearable technology. IEEE Engineering in Medicine and Biology Magazine 22(3), 41–48 (2003)
26. Patel, S., Lai, J.: Who gets to know what when: configuring privacy permissions in an awareness application. In: Proc. CHI 2005, pp. 101–110. ACM Press, New York (2005)
27. Patil, S., Kobsa, A.: Designing with Privacy in Mind. Position paper for Workshop on Awareness Systems: Known Results, Theory, Concepts and Future Challenges. In: Proc. CHI (2005)
28. Pratt, W., Unruh, K., Civan, A., Skeels, M.: Personal Health Information Management. Communications of the ACM, Special Issue on Personal Information Management 49(1), 51–55 (2006)
29. Rogers, M.A.M., Buchan, D.A., Small, D., Stewart, C.M., Krenzer, B.E.: Telemedicine improves diagnosis of essential hypertension compared with usual care. Journal of Telemedicine and Telecare, pp. 344–349 (2002)
30. Schmidtke, H.R.: Aggregations and constituents: geometric specification of multi-granular objects. Journal of Visual Languages & Computing 16(4), 289–309 (2005)
31. Smit, M., McAllister, M., Slonim, J.: Privacy of electronic health records: Public opinion and practicalities. NAEC (2005)
32. Westin A.: How the public views health privacy: survey findings from 1978 to 2005. Privacy & American Business (2005) www.pandab.org/HealthSrvyRpt.pdf