Privacy and Senior Willingness to Adopt Smart Home Information Technology in Residential Care Facilities

K. L. Courtney
University of Pittsburgh, School of Nursing, Department of Health and Community Systems, Pittsburgh, PA, USA

Summary

Objectives: With large predicted increases of the older adult (65 years and older) population, researchers have been exploring the use of smart home information technologies (IT) in residential care (RC) facilities to enhance resident quality of life and safety. Older adults' perceptions of privacy can inhibit their acceptance and subsequent adoption of smart home IT.

Methods: This qualitative study, guided by principles of grounded theory research, investigated the relationship between privacy, living environment and willingness of older adults living in residential care facilities to adopt smart home IT through focus groups and individual interviews.

Results: The findings from this study indicate that privacy can be a barrier for older adults' adoption of smart home IT; however their own perception of their need for the technology may override their privacy concerns. Privacy concerns, as a barrier to technology adoption, can be influenced by both individual-level and community-level factors.

Conclusions: Further exploration of the factors influencing older adults' perceptions of smart home IT need is necessary.

Keywords

Medical informatics, telemedicine, privacy, smart home technology, aged

Methods Inf Med 2008; 47: 76–81

doi:10.3414/ME9104

Introduction

In the United States, the segment of the population that is 65 years and older is expected to grow 54% between 2000 and 2020 and place additional demand on residential care (RC) facilities [1]. In anticipation of this growth, these facilities are adopting smart home information technologies (IT) for the well-being of their residents. Smart home IT are information-based technologies that collect and share resident information with the resident and their health care providers. The purpose of these technologies are to help individuals with tasks they would otherwise be unable to do or to help individuals perform tasks more easily or safely [2]. Examples of smart home IT that are being developed include: emergency help, falls detection, physiological monitoring, cognitive reminder systems, and medication management [3]. Little evaluation research exists on user acceptance and effectiveness of smart home IT in RC facilities [3].

Older adults' perceptions of privacy can inhibit their adoption of smart home IT that could enhance quality of life and increase home safety. Health care providers and researchers cannot assume that health care consumers will necessarily reduce their expectations of privacy based on potential health benefits. Understanding the social forces influencing the willingness to adopt IT is important to the design and implementation of IT [4].

The purpose of this study was to explore the meaning of privacy and how perceptions of privacy by older adults living in residential care facilities might affect their willingness to adopt smart home information technologies. A descriptive, qualitative approach guided by grounded theory principles was undertaken using focus groups and individual interviews.

Background

The relationships between privacy, living environment, and smart home information technologies were explored in this study. The concepts of privacy and living environment have been linked within the literature as have the concepts of living environments and smart home IT. Little prior research however had explored the connections between privacy and smart home IT within different living environments [5].

Living Environment

The meaning of home can be understood as a specific location where privacy and identity are protected; the home as a familiar place of comfort; and the home as the center of everyday experiences [6]. These dimensions of home are linked to familiar routines, physical arrangements and the social structure of the home and are often idealized by residents [6]. RC facilities are designed to provide "home-like" residential environments [7]. Residents' perceptions of "feeling at home" can be related to their perceptions of privacy [8]. Home is part of personal identity and as such a transition to a residential care facility can represent a challenge to one's sense of privacy in many ways [9]. The inclusion of smart home IT in RC facilities could affect privacy through the

rearrangement of personal space to accommodate the technology or through more subtly changing the perception of the home from private space into more public space.

Privacy

Despite many references in the literature, privacy is a multidimensional concept lacking a universal definition [10]. The terms privacy and confidentiality are often used incorrectly as interchangeable terms by health care providers and occasionally within the literature [11]. This study is concerned with an individual's desire and ability to control access to self (privacy) rather than mechanisms designed to respect an individual's privacy expectations (confidentiality).

This subtle distinction between privacy and confidentiality is important as these concepts interact with smart home information technologies in different ways. In the context of smart homes, privacy can affect the willingness of people to participate in smart home projects or their acceptance of certain types of smart home IT and is highly individualized. In contrast, confidentiality in the context of smart home IT is more relevant to the design of the systems and the mechanisms to secure the information that we have been entrusted with. This study focuses on the concept of privacy in a smart home IT project.

Despite a lack of a universal definition for privacy as a concept, there are several descriptive dimensions of privacy which are consistent within the literature and can be useful for examining privacy within residential care settings. Conceptually, privacy concerns are often seen in four distinct dimensions: psychological, social, physical and informational [12]. Each of these dimensions of privacy can result in different personal privacy responses to situations.

In addition to sharing information without consent, it has been suggested that *obtaining* information about a person against their will also constitutes a violation of privacy [12]. Potentially, this aspect of privacy could play a role in an individual's view of information-based smart home IT which can passively collect information, such as one's activity levels, sleeping patterns or treatment adherence, and share it with health care providers or family members. Technology can simultaneously enhance physical privacy through limiting the intrusion of health care providers into the home setting and yet increase the risk of informational privacy violations through inappropriate or unintentional information sharing via the technology [5].

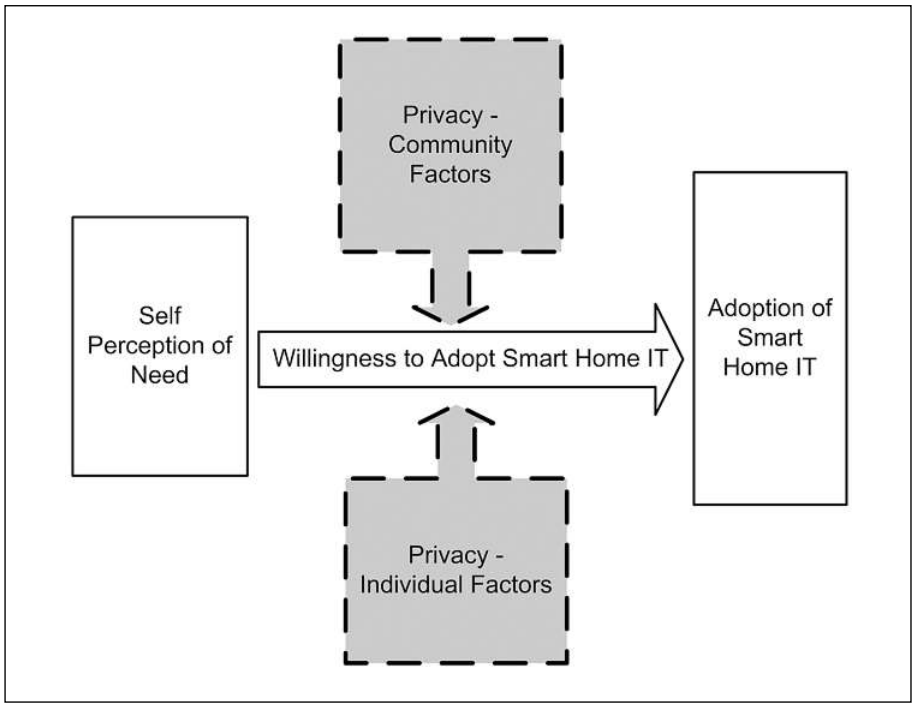

Fig. 1 Privacy as a variable barrier to adoption

Consequences of Perceived Privacy Loss

Within the last decade, concerns about informational privacy and confidentiality have become more prominent. In a survey (n = 92), 80% of respondents indicated they cared "a lot" about their information privacy [11]. Patient's concerns over health information privacy have demonstrable, detrimental effects on their interactions with health care providers. Patient mistrust can lead to the withholding of information; the disclosure of misleading information to their health care providers; or avoidance of the health care system [13].

Smart Home Information Technologies (IT)

Smart home IT are information-based health devices or sensors being installed within private residences and within residential care facilities to enhance residents' quality of life; to help maintain them living at home and to reduce health care costs through prevention and early intervention [14-16].

The ethics literature on home IT suggests that privacy should be an important ethical consideration for implementation and evaluation of these information systems [5, 17]. "The private domain of the home becomes a highly porous, public node where medical information and communication technologies merge" [5, p 140] There is limited existing smart home IT research on the role of privacy in technology decisions. Preliminary research suggests that perceptions of privacy may be a barrier for the adoption of smart home IT [3, 17].

Several studies have suggested that not all older adults or families may uniformly benefit from smart home IT [14, 16].

Knowledge of how privacy concerns affect older adults' willingness to adopt new technologies is one necessary component for identifying which seniors might benefit from the technology. Without this understanding of privacy concerns and willingness to adopt technologies, researchers may not be able to effectively develop smart home IT interventions and target the appropriate users.

This descriptive study explored senior privacy concerns and the willingness to adopt smart home IT within a residential care living environment. Study results are applicable for the development of smart home IT interventions and can inform the practice of health care providers, technology developers, and policy makers.

Methods

Design

Following approval from the Health Sciences Institutional Review Board, data were collected during focus group sessions and during individual interviews. Because the research interest was the meaning of privacy and its effect on older adults' potential adoption of smart home IT, a qualitative approach was used. The goals of qualitative research are description and "understanding and extrapolation to similar situations" rather than prediction or generalization [18]. Data analysis resulted in a description of the perceptions and experiences of privacy and willingness to adopt smart home IT.

Focus groups were selected because we were interested in the complex interaction between privacy and smart home IT adoption within RC facilities. The group interaction could have potentially generated a richer data set because participants could respond to each others' beliefs, feelings and experiences, as well as describe their own. Additional individual interviews were added to the protocol to increase subject diversity and to confirm data saturation (when no new themes emerge) from the focus groups' data.

Sample: Size and Sampling Procedure

After four focus groups (n = 11 unique respondents), data saturation occurred and was confirmed through additional individual interviews (n = 3). Older adults, ages 65 or older living in one of two mid-western U.S. RC facilities were recruited. Residents of these facilities required some assistance with activities of daily living; however were not receiving skilled nursing care. Participants were recruited using flyers in their mailboxes and on bulletin boards within the residence.

Instrument

A semi-structured series of questions guided the facilitator during the focus group and individual interview sessions. Using a constant comparative process during the study, the interim findings generated modifications to the interview guide. Each session began with a discussion about privacy and their residential setting. This was followed by introduction of each technology (bed sensor, kitchen sensor, motion sensor, and fall detection sensor) and a discussion of initial reactions, and whether or not they would be willing to adopt (use) this technology.

Data Collection Procedure

Focus groups and interviews were audio taped and field notes were taken. Discussions lasted until the respondents had nothing new to add, usually lasting 60 minutes. The facilitator summarized the main points from the discussion and thanked the residents for their participation. This summary served as a member check to ensure that we captured the meaning of what the participants intended.

Method of Analysis

Using qualitative approach guided by grounded theory principles, data codes and themes were inductively generated. Following each focus group, transcript data were coded by line and sentence for descriptive and theme codes [19]. Following coding, conceptual maps were created [19]. Interpretations of prior focus group and interview data were validated within each new focus group session. Analysis of the data was performed by the Principle Investigator and two experts (gerontology and informatics) reviewed the coding for validity.

Findings

This study was designed to better understand 1) the relationship between privacy, residential setting and 2) participants' subsequent willingness to adopt smart home IT. The meaning of privacy varied widely among the participants. Initial responses from participants neither uniformly rejected nor accepted the various technologies presented.

The Meaning of Privacy

Personal definitions of privacy ranged from 1) a desire to be alone, 2) a desire to control the information shared with others, 3) a desire to control access to one's personal property, and 4) a desire to protect oneself from identity theft.

Being Alone

Several respondents indicated that privacy was related to being able to be alone or apart from others. One respondent linked being alone with physical separation from others or "not having someone invade your territory". Physical separation from others, such as going to their apartment, was described as a mechanism for achieving privacy.

Information Control

For several participants, the meaning of privacy was tied to the ability to control the content of and recipient of information sharing. Topics that were considered to be private included: sex, feelings, financial

matters, physical condition and visual information (images – still or video).

When you get older, you don't feel that safe on your feet ... And you mean – is it – I have to announce that to everybody? ... I think that's the most private thing that you're really interfering with." Image capture technology prompted strong negative responses from respondents. "You'd feel like a puppet on a string ... I don't want to be – something watching me. I want to be able to do whatever I feel like doing, when I feel like doing, where I feel like doing.

The information recipient was also an important factor in information control. Although in general participants were willing to share their information with family, staff and health care providers, most participants indicated they wanted to be able to choose information recipients.

Property or Territory Control

A few respondents also linked the ability to control access to their property or personal space to their personal definitions of privacy. Personal possessions were considered private.

So in my room I do want my privacy. I want to know that I have my clothes here. I have my jewelry here. I have my little personal things. Yes, that's important to me. I don't want it to be on – anybody can just walk in my room and pick up whatever they'd like. No. I don't like it.

Several respondents indicated the use of physical cues, such as "do not disturb" door hangers or the use of rituals, such as having friends or family call before visiting or making appointments, to control physical access to their rooms and themselves to protect their privacy.

Identity Theft

A few respondents also indicated that their definition of privacy was related to being able to secure their information to prevent identity theft. Concerns about the use of social security numbers as identifiers and computer security were raised as potential threats to privacy. These concerns might also be categorized as confidentiality concerns or concerns about the mechanisms used to protect privacy. But the use of certain unique identifiers, such as social security numbers, may constitute a privacy concern as these identifiers are linked to multiple data sources beyond the smart home.

Table 1 Privacy characteristics

Individual privacy characteristics	Community privacy characteristics
• Desire to be independent	• Crisp boundaries between private and public space
• Desire to control decisions	• Use of behavioral cues (knocking, calling, setting up times in advance)
• Value privacy	• Use of physical cues (door hangers)
• Hyperawareness of technology	• Amount and depth of information shared
• Being "wide open"/willingness to share	• Number in community that share personal information

The Decision to Adopt a Smart Home IT

Rarely did privacy concerns solely dictate respondents' adoption choices. For only a handful of respondents, their privacy concerns clearly guided their rejection of smart home IT. "My privacy is too important to me." Most participants used a pragmatic approach to their technology needs and indicated that their perception of their need for the technology was the most important consideration in the decision to adopt a smart home IT. "Because if I need it, I would get it in a minute, if I could get there before my daughter did." For participants who had privacy concerns about the smart home IT, the privacy concerns were not as important as their perception of their need for the technology. "But as far as privacy is concerned, I think the usefulness of the piece of equipment is the thing that determines that amount of privacy."

Although the willingness to adopt smart home IT was primarily driven by the residents' perceived need for the technology, privacy emerged as a potential barrier to smart home IT adoption. Figure 1 illustrates how privacy moderates the influence of self perception of need on willingness to adopt smart home IT. For some individuals privacy can be a weak barrier to adoption when there are few individual-level and community-level privacy enhancing characteristics. In contrast, for other individuals the presence of many individual and community privacy enhancing factors can present a strong barrier to smart home IT adoption.

Respondents did not uniformly accept the smart home IT shown and most indicated a preference for being able to select only the technology or technologies they perceived they needed. The two technologies mentioned the most often for privacy concerns were the video-based fall detection sensor and the motion sensor. Several factors seemed to influence the privacy concerns about smart home IT. These factors can broadly be divided into two categories: individual-level characteristics and community-level characteristics (Table 1).

Individual-level Characteristics

Individual characteristics are personality or behavior approaches used by the respondents. The presence of these characteristics was varied in both settings. Individual-level characteristics included: a desire to be independent, a desire to control decisions, holding privacy as a value and a hyperawareness of the presence of technology. Respondents who described themselves as having these characteristics were more likely to have privacy concerns regarding the smart home IT presented. In contrast, one individual characteristic was associated with decreasing privacy concerns. This characteristic was a self-description of being "wide open". Participants with this individual characteristic saw themselves as having less privacy concerns overall because of these characteristic. One participant described himself as "I'm not as hyper on the privacy as a lot of the people, I know that. I've left myself wide open."

Community-level Characteristics

In addition to individual-level factors, community-level characteristics also influenced

the privacy concerns of residents (Table 1). Unlike single family home dwellings, residents with residential care facilities have a combination of both private and public spaces within their homes.

> *It's a community and uh, you know, you step out the door and you're in the public area ... the corridors here are not only for you but they're for several other people so you have to respect that. You have to respect the fact that this is not yours totally.*

These community-level characteristics were subtle differences in the way residents described their living environment and their relationships with other residents. In both settings, residents described their relationships with other residents and staff as friendly and as having mutual respect for personal boundaries. Residents from both settings indicated that their privacy needs were respected. In this study, the smart home IT were designed only to be used within the private apartments of the facility and not the shared areas. This restriction in the placement of smart home IT may have influenced the participants' responses regarding community-level privacy factors.

Discussion

Dimensions of Privacy

The findings from this study are consistent with earlier descriptive work on the dimensions of privacy. Respondents in this study used all four of the dimensions of privacy as described by Leino-Kilpi et al. [12]. In their definitions of privacy, the participants indicated concerns about identity (psychological), information recipients (social), physical space and boundaries (physical) and shared information content (informational). In their discussions regarding smart home IT, privacy concerns seemed to be centered in the psychological, informational, and physical dimensions of privacy rather than the social dimension.

Design Implications

Because respondents indicated that the relationship between privacy and smart home IT is multi-dimensional, the possibilities for designing appropriate smart home technology interventions and systems are broader. We recommend that smart home IT be designed so that the residents as collaborative partners in their health care can share contextual information with their health care providers. Information systems can either be designed so that smart home IT algorithms "pull" or prompt residents for information [20] or residents can proactively "push" information to their clinicians as needed [21]. Planned changes in resident activities such as extended trips away from the residence or having house guests are examples of the type of contextual information smart home IT should be designed to capture. Changes in the resident's routine can affect the sensitivity of the system in detecting health problems, but may be considered private information by older adults.

Information sharing will need to be balanced with a resident's desired personal privacy levels. For example, addressing concerns about psychological privacy or the protection of identity may mean smart home IT devices need to be made unobtrusive to the participant and undetectable to the casual observer. In contrast, informational privacy concerns may be addressed through development of resident-designed individual algorithms for information sharing in which the resident controls which information is shared and with whom. Understanding the nature of the privacy concerns of residents will aid researchers, technology developers and policy makers in their practice.

The focus of this study was the exploration of older adults' willingness to adopt smart home IT rather than their actual adoption of the technologies. Future work should re-examine this relationship between privacy, home environment and smart home IT again when the technologies are beyond the development stage and are readily available for individual consumers.

Furthermore, this study assumed that the residents would be the decision makers regarding smart home IT implementation. Potentially, some facilities or families may make this choice for their residents. Additional research is needed to understand the relationship between privacy, living environment and smart home IT when the adoption choice is outside of residents' control or when smart home IT is incorporated into the shared spaces of the facility.

Conclusion

The findings from this study indicate that privacy can be a barrier for older adults' adoption of smart home IT; however, their perception of their need for the technology may override their own privacy concerns. Acceptance of the technology could acknowledge their frailty to themselves and others. If so, those who might benefit the most may be the least likely persons to adopt smart home IT. As one respondent suggested "some people might feel like they're losing a lot of their independence you know, having to rely on somebody and that is hard for a lot of people to accept". This has implications for both the design and evaluation of smart home IT interventions. Further exploration of the factors influencing older adults' perceptions of smart home IT need is necessary.

Acknowledgements

This work was supported in part by the National Library of Medicine Biomedical and Health Informatics Research Training Grant T15-LM07089–14, Alpha Iota Chapter of Sigma Theta Tau, International and the Center for e-Research at the University of Missouri – Columbia.

References

1. Health Resources and Services Administration. Projected Supply, Demand, and Shortages of Registered Nurses: 2000–2020: U.S. Department of Health and Human Services; 2002.
2. Cowan D, Turner-Smith A. The role of assistive technology in alternative models of care for older people. With Respect to Old Age – Research Volume 2. London; 1999. pp 325-346.
3. Demiris G, Rantz MJ, Aud MA, Marek KD, Tyrer HW, Skubic M, et al. Older adults' attitudes towards and perceptions of "smart home" technologies: A pilot study. Medical Informatics & The Internet in Medicine 2004; 29 (2): 87-94.
4. Gortzis LG. Designing and redesigning medical telecare services: A forces-oriented model. Methods Inf Med 2007; 46 (1): 27-35.
5. Bauer KA. Home-based telemedicine: A survey of ethical issues. Cambridge Quarterly of Healthcare Ethics 2001; 10: 137-146.

6. Rousch CV, Cox JE. The meaning of home: How it shapes the practice of home and hospice care. Home Healthcare Nurse 2000; 18 (6): 388-394.
7. Spitzer WJ, Neuman K, Holden G. The coming of age for assisted living care: New options for senior housing and social work practice. Social Work in Health Care 2004; 38 (3): 21-45.
8. de Veer AJE, Kerkstra A. Feeling at home in nursing homes. Journal of Advanced Nursing 2001; 35 (3): 427-434.
9. Hughes M. Privacy in aged care. Australasian Journal on Ageing 2004; 23 (3): 110-114.
10. Scott PA, Valimaki M, Leino-Kilpi H, Dassen T, Gasull M, Lemonidou C, et al. Autonomy, privacy and informed consent 1: Concepts and definitions. British Journal of Nursing 2003; 12 (1): 43-47.
11. Goodwin LK, Courtney KL, Kirby JD, Iannachione MA, Manley T. A Pilot Study: Patients' Perceptions About the Privacy of Their Medical Records. Online Journal of Nursing Informatics 2002; 6 (3). http://www.eaa-knowledge.com/ojni/ni/1002/courtney.htm
12. Leino-Kilpi H, Valimaki M, Dassen T, Gasull M, Lemonidou C, Scott A, et al. Privacy: A review of the literature. International Journal of Nursing Studies 2001; 38 (6): 663-671.
13. California HealthCare Foundation. Medical privacy and confidentiality survey summary and overview. 1999 [cited 10/3/2005]; 1-3]. Available from: www.chcf.org/publications
14. Mangusson L, Hanson E. Supporting frail older people and their family carers at home using information and communication technology: Cost analysis. Journal of Advanced Nursing 2005; 51 (6): 645-657.
15. Stefanov DH, Zeungnam B, Bang W-C. The smart house for older persons and persons with physical disabilities: Structure, technology arrangements and perspectives. IEEE Transactions on Neural Systems and Rehabilitation Engineering 2004; 12 (2): 228–50.
16. Rantz MJ, Marek KD, Aud MA, Tyrer HW, Skubic M, Demiris G, et al. A technology and nursing collaboration to help older adults age in place. Nursing Outlook 2005; 53: 40-45.
17. Mangusson L, Hanson E. Ethical issues arising from a research, technology and development project to support frail older people and their family carers at home. Health and Social Care in the Community 2003; 11 (5): 431-439.
18. Golashani N. Understanding Reliability and Validity in Qualitative Research. The Qualitative Report 2003; 8 (4): 597-607.
19. Miles MB, Huberman AM. Qualitative Data Analysis. 2nd ed. Thousand Oaks, CA: Sage Publications, Inc.; 1994.
20. Struzik ZR, Yoshiuchi K, Sone M, Ishikawa T, Kikuchi H, Kumano H, et al. "Mobile Nurse" platform for ubiquitous medicine. Methods In Med 2007; 46 (2): 130-134.
21. Unruh KT, Pratt W. Patients as actors: The patient's role in detecting, preventing, and recovering from medical errors. Int J Med Inform 2007; 76 (Suppl 1): 236-244.

Correspondence to:
K. L. Courtney
University of Pittsburgh
School of Nursing
Department of Health and Community Systems
415 Victoria Building
Pittsburgh, PA 15261
USA
E-mail: CourtK@pitt.edu