Special issue article

Health Informatics Journal

Health Informatics Journal
18(3) 191–201
© The Author(s) 2012
Reprints and permission: sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/1460458212442933
jhi.sagepub.com
SAGE

Privacy and data security in E-health: Requirements from the user's perspective

Wiktoria Wilkowska and Martina Ziefle
RWTH Aachen University, Communication Science, Germany

Abstract

In this study two currently relevant aspects of using medical assistive technologies were addressed—security and privacy. In a two-step empirical approach that used focus groups (n = 19) and a survey (n = 104), users' requirements for the use of medical technologies were collected and evaluated. Specifically, we focused on the perceived importance of data security and privacy issues. Outcomes showed that both security and privacy aspects play an important role in the successful adoption of medical assistive technologies in the home environment. In particular, analysis of data with respect to gender, health-status and age (young, middle-aged and old users) revealed that females and healthy adults require, and insist on, the highest security and privacy standards compared with males and the ailing elderly.

Keywords

E-health, gender, medical assistive technologies, privacy, security

Introduction

Demographic shifts among industrialized countries are causing fundamental changes in societies and economies. Ageing and population growth have prompted an unprecedented demand on health services, which need to be met by the resources of a shrinking number of young adults. The resulting deficiency in healthcare creates a need for novel technology-assisted solutions to meet the rising difficulties in supporting the constantly growing number of chronically diseased persons, older people, or persons with frail health. Moreover, the increase in the elderly population is forcing the healthcare market to offer senior-friendly products and services related to long-term care, health and wellbeing. Rapid technological advances present novel opportunities to support the ageing and ailing population in maintaining independence and mobility for as long as possible. As the ageing society witnesses these challenging requirements, the concept of ambient assisted living (AAL) has become an attractive notion in recent years. AAL aims to provide whole-time assistance for ailing persons at home in order to help them retain their independence from long-term healthcare

Corresponding author:
Wiktoria Wilkowska, RWTH Aachen University, Theaterplatz 14, Aachen, 52062, Germany.
Email: wilkowska@humtec.rwth-aachen.de

facilities, which, in turn, can help relieve the burden on the healthcare system in the long run. Many practical solutions for AAL can be realized by means of healthcare related technology (E-health) in terms of devices, applications, and services tailored to different types of health conditions. However, despite the potentially high value of these new technological developments for the demands arising from demographic change, the privacy and security of medical information, as well as data handling, is a serious issue[1–4] with considerable consequences for social living and ethical requirements.[5, 6] In order to fully exploit the potential of novel medical technologies, users' perceptions towards security and privacy need to be carefully addressed.

Background/related work

Successful adoption and implementation of these new products and services requires a high user acceptance, which can be achieved by being sensitive to users' special needs and requirements. As personal medical information is being processed and transmitted electronically, possible threats to the protection of individuals' rights to privacy are becoming evident.[7] Moreover, devices designed to assist the elderly in medical monitoring must be carefully examined in light of their security properties as this population is particularly vulnerable. Thus, aside from their possible high practical value for healthcare, E-health products need to take cautionary notes from a human perspective. There is awareness needed that these technologies fundamentally change social and communicative pathways in people's lives and in societies at large.[5, 8] Further, with information and communication technologies (ICT) being available anytime and everywhere, medical technology is being increasingly incorporated in smart homes.[9, 10] Such a permanent presence of technical monitoring, as well as the ubiquitous availability of sensitive data, might be quite critical. On the one hand, positive effects in terms of higher effectiveness, medical treatment and mobility are realized with technical omnipresence, but, on the other hand, perceptions of overstepping personal intimacy limits raise concerns about privacy and data security.[11–13] If concerns outweigh the perceived benefits, the acceptance of medical assistive technology might falter and the consequences could hamper an efficient development and successful rollout of E-health technologies. Therefore, with the ridge between privacy loss and benefit through enhanced medical monitoring, one of the major research intentions in this area is to explore how users perceive different aspects of privacy policy and security of health information within medical technology in order to derive practical implications and research suggestions for E-health acceptance.

Further, given user diversity among potential adopters, the attitudes, needs, wants and technical skills vary considerably within the user community.[14–16] Changing cognitive and affective personal characteristics with age and, in particular, gender are decisive factors for technology adoption and acceptance. Women's self-reported lower competence in handling of, and interest in, technology leads to lower technical skills, particularly as they age.[17, 18] Studies of adoption behaviour of novel technologies in the workplace have also shown that, in general, males tend to be more strongly influenced by their positive attitudes toward technology, while females are more driven by social roles, subjective norms and behavioural control.[19, 20] Although technology usage is no longer restricted to specific groups and penetrates various public and private areas, women are still more reluctant to embrace it than men: for instance, it has recently been shown in a study of the acceptability of invasive medical technology that women—in contrast to men—emphasize usage barriers as more crucial than the expected benefits.[21]

In addition, it is not clear if findings from ICT use can be directly transferred to the field of medical technology—such a transfer is questionable for many reasons. Firstly, in contrast to technology in the workplace, medical technology deals with personal health information that is private and often shared only in confidence with doctors and possibly loved ones. Secondly, medical monitoring is perceived as invading people's intimate and private space, provoking feelings of being constantly controlled;[22] this is often more pronounced in women and in older individuals, especially when medical technology oversteps the personal intimacy limits.[21, 23] Thirdly, medical technology is often considered a 'taboo' associated with disease, making it distinctly different from other ICT used in less sensitive contexts.

Moreover, gender-related differences in adoption behaviours and levels of technical acceptance are an important concern for future developments in the medical technology sector owing to an asymmetrically higher proportion of old, frail women expected to dominate the demographic structure of future societies as a result of the longevity of women compared with men.[24] Considering this, it is extremely important to understand the impact of gender, health and age on technology acceptance, and to identify the specific requirements regarding perceived privacy and data security of E-health technologies.

Research approach

The aim of this study was to examine users' perceptions on privacy and security requirements when using medical technology. Using an exploratory approach, it was intended to understand what specific concerns are associated with these aspects (focus groups) and to identify potential effects of gender and health status on these concerns (questionnaire).

Data were collected from a broad user sample, including healthy and sickly persons. One reason for that was to understand if the acceptance of medical technology depends on health status (assuming that only unwell persons feel it necessary to use E-health and therefore show higher acceptance levels).The second reason referred to an existing knowledge gap between public dispute and potentially ambivalent attitudes towards technology-mediated care concepts in combination with concerns about loss of privacy and security in the population. The understanding of individual beliefs across broad user groups reviewing the facts from different points of view (healthy vs. sick) is certainly of crucial significance as public opinion also considerably impacts the acceptance of future users.

We adopted a mixed methods approach in order to gather different data types that may complement each other. In the first step focus groups were conducted (qualitative data) in order to collect specific details about perceptions of security and privacy in the context of medical technology, i.e.to explore which concepts are associated with these constructs (e.g. data access control, confidentiality of measurement-results). On the basis of these findings a standardized questionnaire was then developed for broader data collection (quantitative data) in order to make more representative statements. Owing to space limitations, we forego a detailed presentation of the qualitative results and report solely on the resulting approach-oriented variables that were incorporated in the quantitative data collection as described hereafter.

Methodology

Data collection

The aim of our *focus groups* was to identify (potential) users' associations with 'security' and 'privacy' when using E-health technologies. In three sessions, carried out in suitable rooms of RWTH Aachen University on two consecutive days, participants shared their ideas, and perceived benefits and concerns about these topics. The participants—invariably native German speakers—were recruited by means of posters in public places and partially by word of mouth using our existing social networks. The groups consisted of women (53%) and men aged between 24 and 73 years. The participants reported quite high educational levels (vocational education: 27%; high school

Table 1. Items for data security and privacy used in the survey

	Item description	Scale
Security requirements (Chronbachs alpha = 0.70)	*'How important are the following security factors when it comes to use medical assistive devices…* *1) The highest possible data protection in general?* *2) The self-determination of data storage and transfer?* *3) The strict data access control?'*	Six-point Likert-scales from 1: 'not at all important' to 6: to 'very important'
Privacy requirements (Chronbachs alpha = 0.87)	*'How important are the following privacy factors when it comes to use medical assistive devices…* *1) Safeguarding of anonymity?* *2) Protection of intimacy?* *3)Confidentiality of measurement-results?* *4) Not stigmatizing design?* *5) Invisibility to outsiders?'*	

degree with abitur[i]: 23%; university degree: 50%) and varying professional fields (social: 32%; medical: 23%; technical: 18%; business: 14%; other: 13%). Four of the 19 persons involved suffered from a chronic disease (e.g. diabetes, cardiovascular disease) and another three reported ailing health; the remaining persons reported to be in good health. The goal was to first obtain insights into common beliefs and cognitive concepts regarding the role of privacy and security for a satisfactory acceptance of medical devices or systems. Methodologically, focus groups allow a deeper insight into the nature of these sensitive topics; the restrictions, however, refer to a comparably small sample size and unbalanced level of education. To validate the representativeness of the findings, outcomes of focus groups were qualitatively analysed and taken as an empirical base for the development of subsequent questionnaires for further quantitative data collection with a larger sample (i.e. the most crucial security and privacy aspects were incorporated as items in the questionnaire; as presented in Table 1).

The *survey* aimed at exploring the prevailing perceptions and assessments of the importance of privacy and security when using E-health technologies. In terms of time, it took place shortly after the focus groups and was arranged in five sections. The first section elicited demographic data (age, gender, education). The second section addressed an individual's experience with technology in terms of usage frequency of ICT devices. The third section included information about health status, various medical devices used (e.g. blood pressure meter) and their perceived usefulness (scale from 1 = not useful to 5 = very useful). The fourth section evaluated the importance of security aspects in medical technologies (e.g. 'How important is the maximum possible data protection to you?') and the last section concerned assessments of privacy relevance (confidentiality, intimacy, anonymity). The relevance of the aspects of security and privacy were measured on a six-point Likert scale (from 1 = not at all important to 6 = very important). Before administering the questionnaire, a linguistic expert verified the comprehensibility and wording of items. Participants took 15–20 minutes to complete the questionnaire. Participation in both the focus groups and the survey was voluntary, and the data were collected in an anonymous way. Ethical approval was not necessary.

Participants

Quantitative data from 104 respondents between 21 and 98 years of age (M = 46.3, SD = 17.8) were analysed. The majority of participants were recruited via advertisements in local newspapers

(57%) and through collaboration with targeted societal groups (e.g. senior citizen home: 28%). The remaining persons were reached through the social network of respondents (7%) and via authors' existing contacts (8%). As intended, the sample covered different population groups including persons with different skills, professional backgrounds and various levels of access to technology. Respondents' socio-economic status (SES) based on income[ii] (small: 46%; mid-range: 28%; high: 15%; very high: 5%; missing data: 6%), education (lower secondary degree: 11%; high school degree: 21%; abitur: 32%; university degree: 36%) and occupational areas (technical: 26%; business: 28%; medical: 12%; social: 8%; other: 26%) differed considerably. This variety in socio-economical background should have assured little or no biased opinions with respect to security and privacy aspects when using E-health technologies. Experience with medical technology use varied as follows: 32% used blood pressure meters; 10% used blood sugar meters; 9% used heart rate monitors; 6% used hearing aids; and 1% used insulin pumps. The perceived usefulness of these medical assistive devices was, in general, rated 'useful' and 'very useful'. Respondents were grouped based on gender (58% female, 42% male) and health status (healthy and ailing) to explore privacy and security perceptions. More than 40% (n = 43) reported suffering from a chronic disease and just as many reported using medical devices. To explore the impact of age, three groups were formed: young users (20–39 years, n = 40; M = 28.3, SD = 4.9), middle-aged users (40–59 years, n = 37; M = 48.6, SD = 5.8) and old users (60–98 years, n = 27; M = 70, SD = 9).

Research variables

The independent variable used was user diversity based on gender and health status in combination with age. The dependent variables were the perceived importance of security and privacy in medical technology, which were revealed as most critical in the focus groups. The greatest concerns for data security applied to data protection in general—a strictly controlled access to, and a self-determined storage and transfer of personal data. In respecting one's privacy when using E-health products, anonymity, confidentiality of the measurement-results and intimacy were revealed to be most crucial (Table 1).

Results

The results of the quantitative analysis are presented descriptively in order to reflect current perceptions and attitudes toward multi-faceted security and privacy aspects. One-way ANOVAs, F-Tests and Spearman's rank correlations are used to determine significant differences between the defined groups. The level of significance is set at 5%. Effects on the less restrictive significance level of 10% are referred to as marginally significant.

Perceptions of data security

As the usage of E-health technologies is mostly directly linked to people with frail health, the first analysis refers to the comparison of perception of security between persons reporting poor health and those with good health. Significant differences appeared in the area of data security: healthy persons perceived the general data protection [F(1,99) = 11.3, $p \leq 0.001$] and the self-determination of data storage and transfer [F(1,99) = 6.7, $p < 0.05$] as much more relevant for E-health usage than persons with poor health (Figure 1A). These results make evident that the value of good health represents, especially for those less healthy, a considerably greater need than the protection and self-determination of digital data, so that they do not pay that much attention to these security aspects. Also, being in poor health requires frequent medical examinations and therefore a high interest in

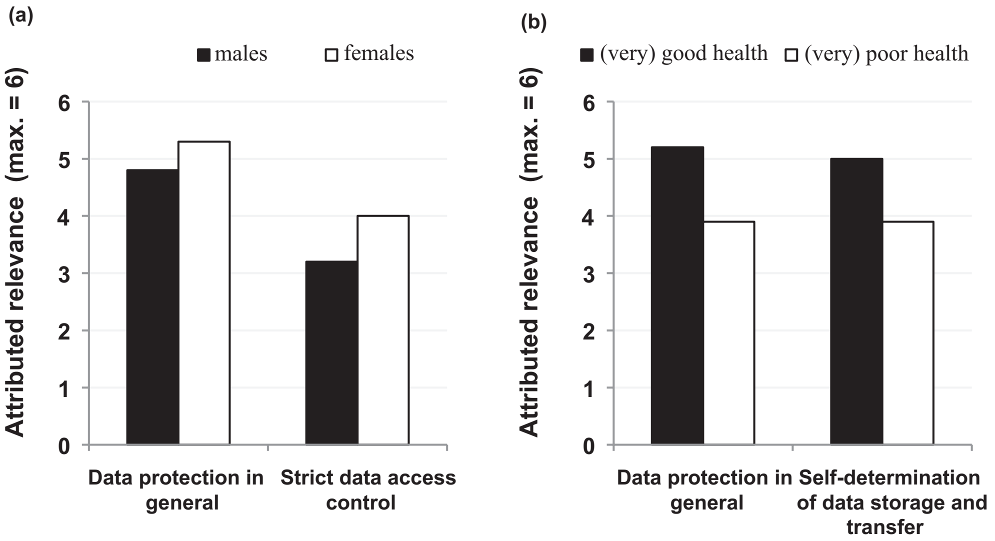

Figure 1. (A) Main effect of gender on security: data protection in general [F(1,99) = 4.1, *p* <0.05] and strict data access control [F(1,98) = 4.7, *p* <0.05). (B) Main effect of health status on data security: data protection in general [F(1,99) = 11.3, *p* ≤0.001] and self-determination of data storage and transfer [F(1,99) = 6.7, *p* <0.05]

quick data access of medical staff. Healthy individuals, in contrast, do not need, or are simply not accustomed to, such a transparency and thus they attach more importance to data protection.

Analysing the gender-related security variables, differences emerged with regard to data protection [F(1,99) = 4.1, *p* <0.05] and the strict control of data access [F(1,98) = 4.7, *p* <0.05]. Women attributed significantly higher relevance to both aspects compared with men (Figure 1B). Overall, as taken from absolute scores, general data protection was judged as more important than strict access control (between ‘moderately’ and ‘slightly’ important). Therefore, women required higher security standards for E-health technology usage and insisted significantly more than men on individually controlled access to personal data.

Perceptions of privacy

Privacy in the context of using E-health assistance comprised requirements of confidentiality, anonymity, intimacy and, not least, invisibility to outsiders. Considering privacy characteristics in the two health groups, significant differences in all examined aspects were revealed. Healthy persons preferred a relatively high degree of confidentiality, anonymity and intimacy. They did not wish their E-health usage and measurement-results to be visible to others and attached great importance to a non-stigmatizing device design. On the contrary, persons with poor health indicated considerably lower privacy demands. From Figure 2 (A, white bars) it becomes obvious that frail persons assessed relevance merely as ‘moderate’ to ‘slightly important’. The differences yielded significant values for anonymity [F(1,98) = 6.6, *p* <0.05], intimacy [F(1,99) =19.4, *p* ≤0.001], confidentiality [F(1,97) = 5.8, *p*<0.05], non-stigmatizing design [F (1,92) = 4.8, *p* <0.05] and invisibility to outsiders [F(1,89) = 12, *p* ≤0.001].

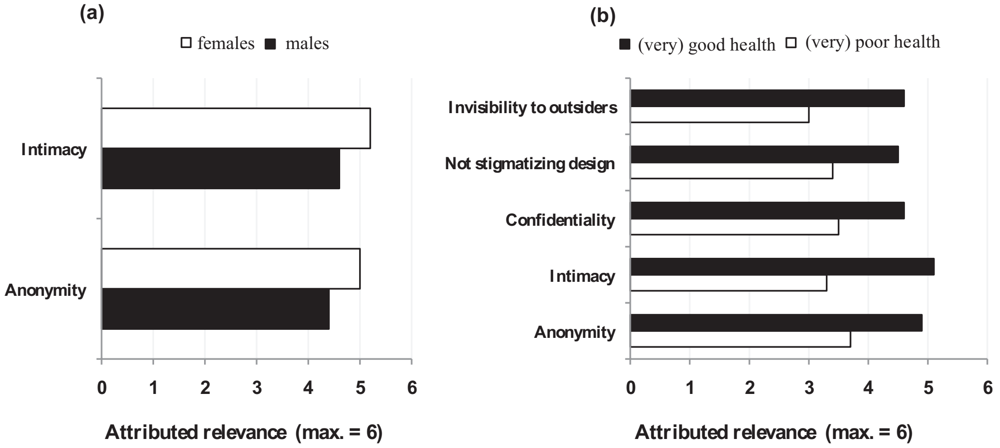

Figure 2. (A) Main effect of gender on privacy aspects: anonymity [F(1,98) = 4.6, *p* <0.05] and intimacy [F(1,99) = 5.3, *p* <0.05]. (B) Main effect of health status on privacy aspects: Anonymity [F(1,98) = 6.6, *p* <0.05], intimacy [F(1,99) = 19.4, *p* ≤0.001), confidentiality of measurement results[F(1.97) = 5.8, *p* <0.05], non-stigmatizing design [F(1,92) = 4.8, *p* <0.05] and invisibility to outsiders [F(1,89) = 12, *p* ≤0.001]

The analysis of gender-specific estimations of privacy concerns revealed differences with respect to anonymity [F(1,98) = 4.6, *p* <0.05] and intimacy [F(1,99) = 5.3, *p* <0.05]. Although both were regarded as quite important overall (Figure 2B), these aspects were considerably more important to women—men, on average, strived less for the possibility of using medical technology in an anonymous and intimate way. Other aspects of privacy were not related to gender.

Age-related inter-relations of research variables

Beyond the clear gender and health status effects, the inter-relation with age has not yet been analysed. As health status is commonly lower in older adults, and as older women are known to be especially reluctant to using novel technologies, this knowledge is of specific interest. We therefore performed correlation analyses separately for three age groups: young, middle-aged and old users. The idea was to explore how gender-specific perceptions of healthy and frail persons in different generations are correlated to privacy and security aspects when using E-health (Table 2).

From the results it is apparent that younger women attributed higher relevance to data protection (r = 0.30, *p* <0.1), confidentiality of measurement results (r = 0.32, *p* ≤0.05) and a non-stigmatizing design (r = 0.28, *p* <0.1) than men did. Also, younger healthy persons attached higher importance to data protection than younger, frail participants (r = 0.29, *p* <0.1). Within the middle-aged group, gender seems to render decisive motivational support to opinions about security and privacy: in contrast to men, women laid higher value on data protection (r = 0.44, *p* <0.01), strict access control (r = 0.56, *p* <0.01), and on anonymity (r = 0.37, *p* <0.05), confidentiality(r = 0.35, *p* <0.05) and invisibility to outsiders (r=0.30, p<0.1). Interestingly, gender effects in the oldest group vanished: older men and women attached the same importance to privacy and security. However, effects of health status were present: healthy older users ascribed higher relevance to intimacy (r = 0.40, *p* <0.05) and invisibility to others (r = 0.44, *p* <0.05). Also, healthy users attached higher importance

Table 2. Spearmann's correlations of research variables in the different age groups (gender: males = 1, females = 2; health status: poor health = 1, good health = 2)

	Young: 20–39 years		Middle–aged: 40–59 years		Old: 60 years and older	
	Gender	Health status	Gender	Health status	Gender	Health status
Data protection	0.30*	0.29*	0.44***	–		
Self–determination of data flow				–		0.38*
Strict access control			0.56***	–		
Anonymity			0.37**	–		
Intimacy				–		0.40**
Confidentiality	0.32**		0.35**	–		0.37*
Non–stigmatizing design	0.28*			–		
Invisibility to outsiders			0.30*	–		0.44**

*p ≤0.1; **p ≤0.05; ***p ≤0.01.

to self-determination of data flow (r = 0.38, p <0.1) and to confidentiality of measurement results (r = 0.38, p <0.1).

Hence, the main actor in perceptions of privacy and security is participants' age. The effect of gender can be traced back to perceptions of young and middle-aged women, whereas health status effects are a result of the perceptions of the oldest people.

Discussion

Successful implementation and adoption of electronic medical devices assisting ageing societies in everyday life has huge potential: for ailing and ageing individuals E-health technology can provide a possibility of retaining mobility and independence at home while at the same time respecting their desire for dignity in ageing. In addition, this could not only enable faster and individually tailored medical help to be triggered in the case of emergencies, but technical medical monitoring would also be enormously beneficial to currently overburdened healthcare systems. However, the development of medical technology must—aside from technical feasibility and medical necessity—consider users' perceptions. A transparent public communication rationale is needed, which informs (potential) users about both assumed benefits and critical aspects. For a higher chance of broad user acceptance and successful adoption, therefore, users' needs, requirements and insights should be considered and incorporated in the implementation of medical technologies.

This research was motivated by a trade-off between the factual necessity of novel medical solutions in the increasingly ageing population and the existing knowledge gap regarding public acceptance of medical technology in different contexts of use and diverse user groups. Two much-discussed current issues of medical technology were addressed—data security and privacy. Apart from the legal and technical aspects of security and privacy, we focused on *the perception* of these aspects, asking under which circumstances users would accept medical technology and assessing if users' gender and health status modulate acceptance. Focus groups clearly uncovered a high awareness of the importance of user-centred medical technology development and a high motivation to express their own opinions and fears connected with usage. This corroborates that current technology development should include users early in order to understand the perceived drawbacks and benefits, and to address their opinions in both development and public communication policy. Furthermore, the questionnaire study revealed distinct user diversity. Women ascribe a higher relevance to the protection and controlled access to their health data, and they insist more than men on using E-health anonymously and in a private manner. This was predominately the case with young and middle-aged women, and less distinct in older women in contrast with the findings on general ICT use. These results clearly indicate the need for personal accounts with password protection in medical devices. Also, fingerprint scans as access control would make the technology more private, secure and trustworthy. Furthermore, this study provides evidence that persons with ailing health attribute lower importance to data security and privacy, which can be a result of the fact that chronically ill individuals consider the importance of fast help and continuous medical monitoring to be higher than their fears of security and privacy loss. However, disregarding healthy individuals' higher concern for the topics discussed would be very counterproductive to effective long-term and widespread adoption of medical technology in private homes. Understanding how people perceive interaction, and how relevant they attribute security and privacy when using E-health paves the way to better usability and consequently to higher acceptance and adoption. This research contributes to this knowledge primarily in two ways. Firstly, it shows that perceived data security and privacy issues mediate the acceptance of medical technology, revealing the relative extent of both factors. Secondly, it corroborates the impact of user diversity and the varying perspectives of different user groups in society.

Nevertheless, even though the findings of the present study confirm outcomes of other recent studies in this context[25–27] we should be aware that the conclusions are not exhaustive. In the following some limitations of the study are outlined which should be addressed in further research. In the focus groups, statements of persons who represented a relatively high level of education (and, as a consequence, possibly higher SES) as a basis for the subsequent survey could be a potential source of bias and we cannot assume that all prevailing aspects of privacy and data security have been covered and examined. Therefore, the extent to which the results can be generalized is limited so that future research needs to include more less-educated persons, as well as to validate the actual findings. Also, even though a considerable portion of the sample was chronically ill, we should be aware that the other portion does not have the same health-related background or experience. Therefore, other influences on their perceptions cannot be excluded (e.g. social esteem, underestimation of the need of medical support). Based on the results, we cannot identify in which respect the reported high importance of privacy issues and data security in medical monitoring represents a global insecurity and whether these systems bring more negative effects than benefits. This further highlights the urgent need for public discussions to concentrate more on straightforward and transparent information and communication policy.

Another possible confounding factor is that this research is (at least partially) restricted to users' imagination of using medical technologies in their private living spaces and is not based on a real experience, which could significantly impact acceptance. People might over-emphasize their sensitiveness towards privacy violations if their judgements rely only on their imagination of using medical technology.[28] Thus, future studies need to integrate a real user experience into acceptance evaluation. In order to examine how persons actually behave in technology-assisted environments, an experimental space is necessary that simulates such technologies at home. Only users'active interaction with a technology-enhanced environment can make them 'feel' its real impact and would possibly allow unbiased statements about factors influencing acceptance.[29]

In summary, medical assistive technology in the daily life of our ageing societies is very promising and brings many benefits. Adoption, however, is not self-evident and requires a high level of acceptance among (potential) users. In the current discussions, aspects of data security and privacy are of especially high interest as they may represent potential obstacles in a successful adoption and proliferation of E-health. The success is mediated by acceptance, which can be only achieved through inclusion of a wide circle of addressees in the research, through identification of weak points and elaboration of effective solutions, and through a consequent realizing of the knowledge gained in technical development and production.

Funding

This research was supported by the Excellence Initiative of the German federal and state governments.

Notes

i. German university entrance qualification
ii. Income classification (per year):*small:*< 20.000 Euros; *mid-range:* 20.000 – 40.000 Euros; *high:* 40.000 – 70.000 Euros; *very high:*> 70.000 Euros

References

1. Meingast M, Roosta T and Sastry S. Security and privacy issues with health care information technology. *Conf Proc IEEE Eng Med Biol Soc* 2006; 1: 5453–5458.
2. Shmatikov V. Anonymity is not privacy: technical perspective. *Commun ACM;* 2011; 54: 132–132.
3. Reynolds B, Venkatanathan J, Gonçalves J and Kostakos V. Sharing ephemeral information in online socialnetworks: privacy perceptions and behaviours. *Proc of Interact* 2011; 3: 204–215.
4. De Vimercati SDC, Foresti S, Livraga G and Samarati P. Protecting privacy in data release. In: Aldini A and Gorrieri R (eds) *FOSAD VI*. Berlin: Springer, 2011, pp.1–34.
5. Lahlou S. Identity, social status, privacy and face-keeping in digital society. *Soc Sci Inform* 2008; 47: 299–330.
6. Anderson JG. Social, ethical and legal barriers to E-health. *Int J Med Inform* 2007; 76: 480–483.
7. Choi YB, Capitan KE, Krause JS and Streeper MM. Challenges associated with privacy in health care industry: Implementation of HIPAA and the security rules*. J Med Syst* 2006; 30: 57–64.
8. Rogers EM. *Diffusion of Innovations*, 4th ed. New York: The Free Press, 1995.
9. Meyer S and Mollenkopf H. Home technology, smart homes, and the aging user. In: Schaie KW, Wahl H-W, Mollenkopf H and Oswald F (eds). *Aging Independently: Living Arrangements and Mobility.* New York: Springer, 2003, pp.148–161.
10. Grabner-Kräuter SD and Kaluscha EA. Empirical research in on-line trust: a review and critical assessment. *Int J Hum Comput Stud* 2003; 58: 783–812.
11. Caine KE, Fisk AD and Rogers WA. Benefits and privacy concerns of a home equipped with a visual sensing system: a perspective from older adults. *Proc. Hum Factors Ergonom Soc* 2006; 180–184.
12. Corritore CL, Kracher B, Wiedenback S and Marble R. Foundations for trust for E-Health. In: Ziefle M and Röcker C (eds) *Emerging healthcare systems*. Hershey, PA: IGI Global, 2011, pp.49–75.
13. Petković M and Ibraimi L. Privacy and security in e-Health applications. In: Ziefle M and Röcker C (eds) *E-Health, Assistive Technologies and Applications for Assisted Living: Challenges and Solutions.* Hershey, PA: IGI Global, 2011, pp.23–48.
14. Wilkowska W and Ziefle M. User diversity as a challenge for the integration of medical technology into future home environments. In: Ziefle M and Röcker C (eds) *Human-Centred Design of eHealth Technologies.Concepts, Methods and Applications.* Hershey, PA: IGI Global, 2011, pp.95–126.
15. Arning K and Ziefle M. Different perspectives on technology acceptance: the role of technology type and age. In: Holzinger A and Miesenberger K (eds) *HCI for eInclusion.* Berlin: Springer, 2009, pp.20–41.

16. Wilkowska W and Ziefle M. Which factors form older adults' acceptance of mobile information and communication technologies? In: Holzinger A and Miesenberger K (eds) *HCI for eInclusion*. Berlin: Springer, 2009, pp.81–101.
17. Schumacher P and Morahan-Martin J. Gender, internet and computer attitudes and experiences. *Comput Hum Behav* 2001; 17: 95–110.
18. Mitzner TL, Boron JB, Fausset CB, et al. Older adults talk technology: technology usage and attitudes. *Comput Hum Behav* 2010; 26: 1710–1721.
19. Morris MG, Venkatesh V and Ackerman PL. Gender and age differences in employee decisions about new technology: an extension to the theory of planned behavior. *IEEE T Eng Manage* 2005; 52: 69–84.
20. Wilkowska W, Gaul S and Ziefle M. A small but significant difference – the role of gender on the acceptance of medical assistive technologies. In: Leitner G, Hitz M and Holzinger A (eds) *HCI in Work & Learning, Life & Leisure.* Berlin: Springer, 2010, pp.82–100.
21. Ziefle M and Schaar AK. Gender differences in acceptance and attitudes towards an invasive medical stent. *eJHI* 2011; 6: 1–18.
22. Montague E, Kleiner BM and Winchester WW. Empirically understanding trust in medical technology. *Int J Ind Ergonom* 2009; 39: 628–634.
23. Kowalewski S, Wilkowska W and Ziefle M. Accounting for user diversity in the acceptance of medical assistive technologies. In: Szomszor M and Kostkova P (eds) Electronic Healthcare. Lecture Notes of the Institute for Computer Science, Social Informatics and Telecommunication Engineering 69. Berlin: Springer, pp.175–183.
24. Austad SN.Why women live longer than men: Sex differences in longevity. *Gender Med* 2006; 3: 79–92.
25. Ziefle M, Röcker C and Holzinger A. Medical technology in smart homes.Exploring the user's perspective on privacy, intimacy and trust. IEEE 35th Annual Computer Software and Application Conference Workshops 2011; 410–415.
26. Röcker C and Feith A. Revisiting privacy in smart spaces: Social and architectural aspects of privacy in technology-enhanced environments. In: *Proceedings of the International Symposium on Computing, Communication and Control* 2009; 201–205.
27. Ziefle M, Himmel S and Wilkowska W. When your living space knows what you do: Acceptance of medical home monitoring by different technologies. In: Holzinger A and Simonic K-M (eds) *Human-Computer Interaction: Information Quality in eHealth.* Berlin: Springer, 2011, pp.607–624.
28. Cvrcek D, Kumpost M, Matyas V and Danezis G. A Study on the Value of Location Privacy. In: Proceedings of the ACM workshop on Privacy in the Electronic Society. New York: ACM, 2006, pp.109–118.
29. Klack L, Schmitz-Rode T, Wilkowska W, Kasugai K, Heidrich F and Ziefle M. Integrated home monitoring and compliance optimization for patients with mechanical circulatory support devices (MCSDs). *Ann Biomed Eng* 2011; 39: 2911–2921.