Perception of Privacy and Security for Acceptance of E-health Technologies

Exploratory analysis for diverse user groups

Wiktoria Wilkowska
Communication Science, RWTH Aachen
Human Technology Centre
Aachen, Germany
wilkowska@humtec.rwth-aachen.de

Martina Ziefle
Communication Science, RWTH Aachen
Human Technology Centre
Aachen, Germany
ziefle@humtec.rwth-aachen.de

***Abstract*—The present study explores perceived relevance of security and privacy aspects in different user groups and assesses the predictive power of these attributes on acceptance of medical assistive technologies. Based on previously conducted focus groups a questionnaire was developed and quantitative data from N = 104 persons were analyzed. In a descriptive manner opinions of adults in all stages of life (age groups from young, middle-aged to older people) as well as gender- and health-related are presented and discussed with regard to those characteristics, and differences between the groups are disclosed. In multivariate regressions follows the analysis of most predictive security and privacy attributes for the acceptance (i.e. perceived usefulness) of E-health technologies. Results show that both security and privacy aspects play an important role for acceptance and usage of medical assistive technologies.**

Keywords: security, safety, privacy, E-health technologies, acceptance, user diversity

I. INTRODUCTION

Faced with current demographical transition and the resulting deficiency in healthcare sector, new solutions are needed to meet the arising difficulties in supporting chronically diseased, older, or persons with frail health. The rapid technical development at the same time opens up new opportunities, which could be used to support these people in maintaining their independency and mobility in every day life in spite of their restrictions and handicaps.

As the graying society evinces more challenging needs and requirements, the concept of ambient assisted living (AAL) was brought to life in recent years. The idea thereby is to provide whole-time assistance for older, chronically diseased, and persons with frail health in their own home environment in order to maintain their independency from healthcare facilities (e.g., nursing home), and in the long run, to relieve step by step the overburdened healthcare system. Practicable solutions for supporting the elderly and ill individuals in place are realized by means of health care related technology (= E-health) in terms of particular devices, applications, components and services geared to the special needs or demands of the individuals. The question is, does the target group agree and accept such solutions?

Beyond their undisputed value for health care and an efficient as well as time-critical medical supply chain, there are some cautionary notes from the human perspective, which will rely on these technologies. We should be aware that these technologies do fundamentally change the nature of social, economic and communicative pathways in societies, and that they bring essential changes to our lives (e.g., [1], [2]). Communication and information technologies are present everywhere and at any time, and they overcome physical as well as mental borders ([3]). Mobile medical technology is increasingly incorporated in smart homes (i.e. walls or furniture) as well as in smart clothes ([4], [5]). Such devices might overstep personal intimacy limits, raising concerns about privacy, data security and loss of control [6], [7]. Sensitive and detailed information regarding various topics is available everywhere and anytime. This implicates both, positive effects in terms of productivity, mobility and growth, but also negative effects: Users may be concerned about violations of privacy and data security [8], [9], [10] as well as infrastructure constraints. Current developments require a high acceptance and impose high responsibility to all persons and organizations involved, i.e. users, decision makers, technical designers and developers, but also industry, economics and legislation.

While there is an ongoing vivid discussion from the technical perspective on data safety, privacy and security (for an overview see [11]), only very few research papers specifically deal with the nature of perceived privacy and security concerns in the medical sector. This seems a critical research issue, as the full acceptance of medical technology is especially sensitive.

Generally, the understanding of factors that influence technology acceptance is essential for its successful adoption [2]. With respect to common information and communication technology, models have been worked out to understand these factors and to predict technology acceptance (e.g., [12], [13], [14]). The Technology Acceptance Model (TAM) [13] and its further development named Unified Technology Acceptance and Use of Technology (UTAUT) [14], build the theoretical framework in this research. TAM was originally developed to understand acceptance of information technology and presented as the key components the perceived ease of using a system and the perceived usefulness. However, considering the increasing complexity of technical systems, the diversity of

978-1-936968-15-2 © 2011 ICST

DOI 10.4108/icst.pervasivehealth.2011.246027

users as well as their confrontation with different using contexts (e.g., informative, communicative, entertaining, job-related) additional aspects need to be included into the analyses in order to better understand the acceptance pattern. Hence, in addition to user characteristics like gender, age, technical experience, and voluntariness of system usage also expected performance and effort as well as social influence had been considered in the comprehensive UTAUT model [14].

In recent years technology acceptance is explored especially within the medical context [7], [15], [16]. Outcomes show, that it is highly questionable that acceptance for E-health technologies can be fully understood on the base of prevailing knowledge of technology acceptance drivers so far. Acceptance with regard to medical technology usage – concerning such sensible topic as the own health – might be a much more complex phenomenon, where considerations like privacy and system security can be (partially) decisive for the usage behavior. In the current research we thus explore what people associate with privacy and security of E-health technology usage, and how do they assess the relevance of their previously identified related aspects.

II. RESEARCH APPROACH

The aim of the study was to examine users' perception of privacy and security requirements when using popular medical technology devices (e.g., blood pressure meter, blood sugar meter, insulin pump). Using an exploratory approach, it was intended to learn which attitudes, demands, fears, and hopes are associated with these aspects and how they might differ depending on user diversity.

In this context, it is often argued that healthy persons cannot "feel" the importance and the necessity of medical technology, as they are not truly concerned. Even if it is naturally acknowledged that people suffering from a chronic disease do have a specifically elaborated perspective on this topic, there is though an enormous gap in the knowledge about public discourse and potential ambivalent attitudes to technology-mediated care concepts in combination with concerns about loss of privacy and security. The understanding of individual beliefs and general attitudes are thus of crucial significance as the public opinion also considerably impacts the cognitive mind setting of future users.

Therefore, in this research, we examined a broad user sample and addressed specifically privacy and security issues in medical technology. Methodologically, we used a mixed methods approach in order to collect different types of data that may complement each other and allows us a deeper understanding of the nature of potential concerns. In the first step focus groups were conducted for collecting specific details about the perceived security and privacy aspects regarding acceptance and usage of medical assistive devices (qualitative data). Based on the results a questionnaire was then developed in order to collect data from a larger sample (quantitative data).

III. METHODOLOGY

A. Qualitative Data Collection

In the first step of the research focus groups were conducted in order to identify, which concepts (potential) users associate with the terms "security" and "privacy" when using medical assistive technologies (= E-health technologies). The participants – invariably German native speakers – were recruited by means of posters in public places as well as using authors' existing social networks. Spread across the groups, four persons suffered from chronically disease (e.g., diabetes mellitus, cardiovascular disease), and another three participants reported poor health. In three consecutively proceeded sessions (focus groups) overall nineteen persons participated and brainstormed about the mentioned topics sharing their ideas with the others in the subsequent discussions. The groups consisted of different aged persons of both gender groups, with diverse educational, social and professional backgrounds (physicians, teachers, engineers, economists, etc.) as well as with diverse levels of technical experience:

- The first focus group consisted of seven persons, mostly students, aged between 24 and 29 years (M = 26.8, SD = 1.5), 57% female;
- The second focus group was composed of six females covering the age range from 60 to 68 years (M = 63.8, SD = 3.6);
- And, in the third focus group participated six 67 to 73-year-old males (M = 69.2, SD = 2.1).

The goal of the focus groups was to gather general opinions and perceptions regarding privacy and security issues when using technologies – in the first instance technology in general, but the special emphasis applied to medical devices or systems. With respect to age and gender, participants within the groups were homogeneous and between the particular groups heterogeneous. This design based on persons' commonalities should have promoted lively discussions, and, the differing groups structure in age, gender and health status should have ensured that diverse (potential) users talk and express their viewpoints about the mentioned topics. The discussions were guided and encouraged by an experienced moderator and followed prompt after time intervals of individual work given to reflect about the particular subject matters (free associations, e.g., "What does mean to you 'security' while using medical technologies? Please note down in keywords every idea, which springs to your mind within the time of one minute."). Accompanying short questionnaire collecting demographical data, details about the health status and technology usage was used. All discussions were audio-recorded and the results of brainstorming were collected and visualized on a pin board prior to the group discussions.

The general aim was to obtain first insights into the in users existing beliefs or concepts regarding the role of privacy and security for satisfactory acceptance, and to lay a foundation for developing the questionnaire and a quantitative data collection. The analysis of the qualitative data was carried out in consideration of number and elaborateness of the topics discussed. Due to space limitations, we forego a detailed presentation of the qualitative results and focus for reasons of representativeness primarily on the quantitative outcomes regarding the main points of interest.

B. Quantitative Data Collection

With the next step a questionnaire was designed in order to explore the in the population prevailing perceptions and

assessments of privacy and security when using E-health devices. The subjective data were collected in a random sample of N =104 adults between the ages of 21 and 98 years of age in order to learn and reflect the opinions regarding those aspects of people at all stages of life.

The questionnaire was arranged in five sections. The first part included demographic data with respect to participants' age, gender, educational level and profession. The second section applied to person's experience with technology in general. Thereby usage-frequency of popular information and communication devices (personal computer, mobile phone, video/digital camera, navigation system/GPS) was assessed. The next part of the questionnaire included information about the health status, general dealing with illness, usage of medical assistive devices (e.g., blood pressure meter, blood sugar meter, insulin pump), and the perceived usefulness (PU) of these (assessments on a five-point Likert scale from 1 = "not useful at all" to 5 = "very useful"). The forth section focused on security and safety aspects when using medical technologies. The data were collected in two different formats. One referred to perceived advantages and disadvantages of using E-health technology, whereby respondents had to express their degree of (dis-)agreement on a five-point Likert scale ranging from 1 (do not agree at all) to 5 (fully agree), whereas the estimations of relevance were arranged at six-point Likert scale ranging from 1 (not important at all) to 6 (very important). The items referred to both system-/data-security (e.g., "How important is the maximum possible data protection to you?") and the perceived safety with respect to the health monitoring (e.g., "I would use medical technology device(s), because storage of my health data would enable a quick access in case of emergency"). Finally, the items of the last part of the questionnaire assessed the relevance of the in focus groups identified aspects of privacy when using medical assistive devices (e.g., discreetness, intimacy, anonymity).

Before administering, linguistic expert verifying comprehensibility and wording of items revised the questionnaire, and it was pretested by a sample of different aged adults (n = 5). The fill in of the final version took 15-20 minutes.

C. Participants

Qualitative data from 19 younger and older adults participating in three focus groups (as described above), and quantitative data from 104 younger, middle-aged and elderly persons who were respondents in the questionnaire study, were collected and analyzed. Participants were reached on different ways using advertisement in local newspapers, authors' existing contacts (e.g., senior-citizen home) as well as social network of respondents, which were asked to pass the information of recruitment on to their friends and/or family members. For the evaluation of the quantitative study participants were spitted in six age groups as follows:

- The first age group comprises n = 25 young persons aged between 21 and 29 years of age (M = 25.2, SD = 2.6), 60% females;
- The second age group consists of n = 15 younger middle-aged adults within the age range 30 to 39 years of age with the mean age of M = 33.5 (SD = 3.1) and the proportion of 40% female and 60% male respondents;
- The third age group is composed of n = 21 middle-aged 40 to 49-years-olds (M = 44.1, SD = 2.7), whereby 76% females and 24% males participated;
- The forth age group includes n = 16 older middle-aged persons at age between 50 and 59 years (M = 54.4, SD = 2.9; 56% female respondents);
- The fifth age group consisting of n = 16 older adults aged between 60 and 69 years of age (M = 64.8, SD = 2.6) was gender-balanced with 50% women and 50% men;
- And the sixth age group form n = 11 elderly females (54%) and males (46%) from the age of 70 years upwards reaching the mean age of M = 77.6 (SD = 9.6).

This partition was created in order to reflect the prevailing opinions, attributions and attitudes in the population. As each age group adapted technology at different stages of development, it was of interest, if peoples' perceptions regarding security and privacy using medical technologies differ in those groups. Age itself is only a carrying variable reaching a mean value of M = 46.3 (SD = 17.8) in the whole sample. Gender (58% female participants) is considered in the analyses due to some substantial differences regarding technology usage as present in current literature (e.g., [7]). And also, the sub-division of the sample in (very) healthy (80%) and rather sickly (20%) respondents, based on self-reports, is carried out, as E-health technology usage might have a lot in common with the current health condition. Thus, different ages and gender together with participants' referred, subjective perceived health status represent the user diversity of our society and would be a permanent part of our descriptive analyses.

D. Research Variables

One of the main objectives of this study is the perceived security when using medical assistive devices. Based on the discussions resulting in focus groups there are rather more trends within this topic. S*ystem-security* and *data-protection* are aspects of technology usage, where people might be concerned about the reliability of the device or fear the possible incorrect information or inaccurate measurement results (item-descriptions are given in Table 1). Other trend is the *perceived safety* regarding the own health, i.e. the feeling of being safe when monitoring – whether prophylactic or in terms of aftercare – critical health parameters by means of medical devices. Moreover, *perceived security advantages* brought by E-health technology (e.g., medication reminder) are added to the debate over its acceptance and usage.

The second object of interest in this research is the *perceived privacy* when using E-health products. We examined in addition to the general perceived relevance of privacy (ratings from 1 – not important at all – to 6 – very important), the role and importance of previously identified aspects of privacy, like – among others – anonymity, discreetness, and intimacy (see Table 1).

TABLE I. RESEARCH VARIABLES

Object of research	Topic	Item description
Security	System security	- Lacking reliability of the system, - Worry about measurements' inaccuracy / misleading information,
	Data protection	- Data protection in general, - Self-determination of data storage and transfer, - Strict data access control
	Health safety	- General safety feeling when using E-health technologies, - Regular health parameter monitoring, - Health data collection and quicker access in case of emergency
	Perceived security advantages	- Feeling safe in spite of illness / disease, - Additional advantages due to supplementary functions (e.g., medication reminder)
Privacy	Perceived privacy of…	- Usage in general,
	Privacy requirements	Anonymity, intimacy, discreetness, not stigmatizing design, invisibility to outsiders / third persons, worry about a permanent surveillance

As already indicated, the opinions about security and privacy in association with E-health technologies usage are analyzed in this research from three different angles: (1) overview in the whole range of adulthood (age groups), (2) gender-specific perception (males vs. females), and (3) in dependency on the self-reported health status ((very) good health vs. (very) poor health). Respondents' opinions are showed by means of assessments of perceived advantages and disadvantages of E-health usage, as well as regarding the attributed relevance of the identified security and privacy variables. Additionally, the association structure of those attributes with perceived usefulness as an indicator for acceptance is examined.

IV. RESULTS

The results of the quantitative analysis are presented in descriptive matter in order to reflect current perceptions and attitudes toward multi-faceted security and privacy aspects regarding medical assistive technologies in different age stages. One-way ANOVAs and T-tests are used to determine significant differences between age, gender and health-related groups. To specify the best predictors for acceptance of E-health technology usage multiple linear regression analyses are conducted.

The level of significance is set at 5%, as it is usually the case in social science. Though, as we pursued an exploratory approach and as the topic is quite complex, plus, as the users, which were addressed, are quite divers, we also considered outcomes within the less restrictive significance level of 10% as marginally significant.

The result section is arranged in three parts: in the first step we describe security and safety aspects perceived as meaningful for acceptance of medical technologies; in the second part we present the distribution of different facets of privacy in the same context; and the third section demonstrates how security and privacy are related to perceived usefulness (= acceptance) of E-health technology usage. Because of space reasons only statistically significant results are illustrated.

A. Perceived Security and Safety when Using E-health Technology

As already mentioned in the methodology section, the perceived security of medical technology usage is multi-layered and thus in our analysis it is partitioned in system security, health safety, data protection and additional security advantages.

Analyzing the distribution of the particular variables statistically significant age groups differences result only for the attributed relevance of general data protection ($F(5,94) = 2.7$; $p < 0.05$) and marginally for the assessment of system reliability ($F(5,95) = 2.1$; $p = 0.07$). As it is apparent in Figure 1 (right) people in almost all ages perceive protection of their personal data as (very) important – the groups' mean values lie mostly in the top third of the scale. Solely those over 70 years olds attribute with an average of $M = 3.8$ ($SD = 2.1$) out of maximum 6 points the data protection as not too important. Additionally, respondents' assessments of lacking system reliability tend to differ over the years, whereby younger users more frequently as the middle-aged and older ones perceive unsatisfactory system reliability as reason for not using E-health technology (Figure 1 left). Besides, persons in different ages do not differ in their opinions with respect to other – in Table 1 reported – security advantages when using E-health, whereby the means for health safety reach overall higher importance and higher assessment as the system security.

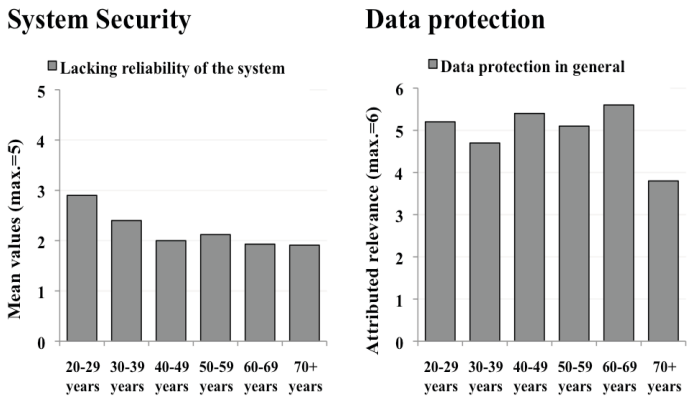

Figure 1. Age group differences regarding security aspects in medical technology usage

What about the gender? We found meaningful gender-specific differences with regard to data protection ($T(1,98) = -2$, $p < 0.05$) and strict control of data access ($T(1,97) = -2.2$, $p < 0.05$). In both, the female part of the sample reports significantly higher relevance values than males (Figure 2 right). In contrast, men tend more than women to perceive the advantage of regular health control using medical devices as valuable ($T(1,100) = 3.3$, $p = 0.070$; Figure 2 left). The estimations for the other security-related variables are not significantly differing in the both gender groups.

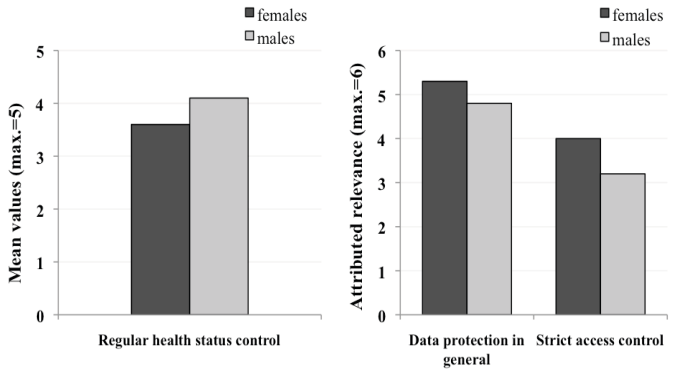

Figure 2. Gender differences in security aspects for medical technology usage

Furthermore, as E-health technologies usage is mostly related to a frail health condition, it is of interest if there are any differences in opinions regarding security between persons reporting poor or very poor health and those with (very) good health. Under this condition significant differences in the area of data protection appear: healthy persons perceive the general data protection ($T(1,98) = 3.4$, $p \leq 0.001$) as well as the self-determination of data storage and transfer ($T(1,98) = 2.6$, $p < 0.05$) as much more relevant for E-health usage than persons with poor health; Figure 3 (right) shows the according mean values for both groups. Apparently, good health represents a greater need in comparison to the protection and self-determination of personal data, so that less healthy persons do not pay that much attention to the secure storage and transfer.

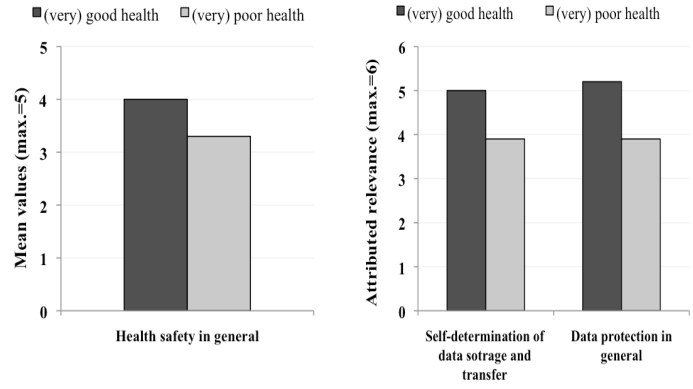

Figure 3. Differences in security aspects comparing persons with good and poor health conditions

Additionally, there are marginally significant differences between the health-related groups regarding the general health safety ($T(1,100) = 1.9$, $p < 0.1$): healthy people tend stronger than sickly to perceive a high advantage in using medical devices in order to monitor their general health condition (Figure 3 left).

B. Perceived Privacy when Using E-health Technology

Privacy in context of using E-health assistance comprises varying interpretations and involves closely related concepts (= privacy requirements) like discreetness, anonymity, intimacy and not least invisibility to others. The question is how diverse respondents assess their importance for acceptable technology.

When asked, persons in all age groups refer a relatively high relevance of these aspects (the mean values lie between 3.8 and 5.2 out of maximum 6 points for the highest importance) and there are not meaningful differences about this topic in various ages (n.s.). Moreover, responses regarding a feeling of permanent surveillance and the perception of E-health technology usage as disadvantage (because other persons would notice the illness) reach in the different age groups overall means of $M = 2.3$ ($SD = 1.3$) and $M = 2.2$ ($SD = 1.3$), which with the maximum range of 5 points indicates rather lower perception of intrusion into ones private sphere. Here too, the differences are not statistically significant (n.s.). These results let conclude that regardless of persons' age, privacy is perceived as fundamental for the acceptance and usage of medical technology.

However, according to gender-specific estimations of privacy aspects, differences with respect to the safeguarding of anonymity ($T(1,97) = -2.1$, $p < 0.05$) and intimacy ($T(1,98) = -2.3$, $p < 0.05$) when using E-health technology between the opinions of men and woman emerge. As presented in Figure 4, these aspects are considerably more important to the female part of the sample reaching mean values over 5 out of 6 possible points on the scale, whereas males – although still quite high – pay less attention than woman to the possibility of using medical technology in an anonymous and intimate way. The remaining aspects of privacy do not differ within the gender groups.

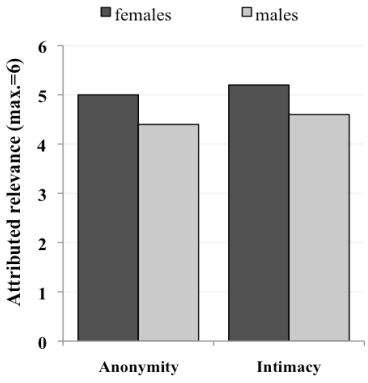

Figure 4. Gender differences in privacy aspects for medical technology usage

In contrast, considering privacy characteristics from the health-related point of view, more significant differences become visible. People with good health condition prefer relatively high degree of discreetness, anonymity and intimacy. They do not wish their E-health technology usage to be visible to others, and attach great importance to a not stigmatizing design of the devices. On the contrary, persons with rather poor health status pay decidedly less attention to those privacy attributes. Looking at the grey bars in Figure 5 it's obvious that the mean values in the group with rather poor health do not even reach the number 4 on the scale, oscillating between the expressions "moderately important" and "of little importance".

The differences are confirmed in unpaired two-sample T-tests: discreetness T (1,96) = 2.4, $p < 0.05$; anonymity T (1,97) = 2.6, $p < 0.05$; intimacy T (1,98) = 4.4, $p \leq 0.001$; not stigmatizing design T (1,91) = 2.2, $p < 0.05$; and, invisibility to outsiders T (1,88) = 3.5, $p \leq 0.001$. Additionally, the results reveal that those with frail health in comparison to healthy people tend to feel less worried about the permanent surveillance while parameter monitoring (T (1,95) = 2.1, p = 0.058).

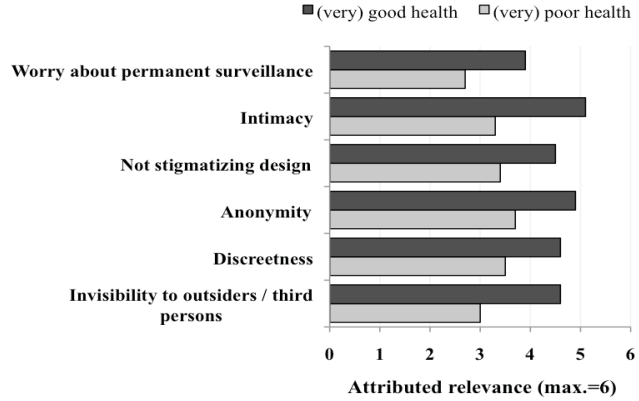

Figure 5. Differences in privacy aspects comparing persons with good and poor health conditions

C. *How Are Security and Privacy Aspects Associated to Acceptance of E-health Technology*

After description of the distribution of security and privacy aspects in different user groups of the sample, in this section we focus on the relationship between the described variables and acceptance in terms of perceived usefulness of medical technology. The decisive question is now: if and to which extent do security and privacy issues account for the acceptance and usage of E-health technologies? For the analysis of the association structure between the predictors (security aspects; privacy aspects) and criterion (perceived usefulness of E-health technology) a multiple linear regressions were conducted.

In order to specify, which of the security aspects have the most explanatory power stepwise regression method was chosen. The analysis revealed that three of the security variables have been included into the regression model (see upper part of Table 2): (1) the general health safety feeling when using medical technologies, (2) health data collection and quicker access in case of emergency (both health safety), as well as (3) lacking system reliability (system security). These health safety and system security aspects explain 38.3% of the variance and result in the following regression equation:

Security = 2.8 + 0.3*general safety feeling + 0.1*quicker data access in case of emergency – 0.2* lacking system reliability

With respect to privacy variables – as presented in the lower part of Table 2 – in the stepwise analysis two characteristics were added in the regression model: (1) worry about a permanent surveillance when regularly monitor health parameters, and (2) protection of intimacy by E-health technology usage. The privacy aspects contributing to the variance-explanation of perceived usefulness are given below in the regression equation (in parentheses: percentage of the explained variance):

Privacy (19.2%) = 4.2 – 0.3*worry about permanent surveillance + 0.1*protection of intimacy

TABLE II. RESULTS OF MULTIPLE STEPWISE REGRESSION ANALYSIS (N = 104; VIF = VARIANCE INFLATION FACTOR < 5)

Crite-rion	Best predictors	Adj. R^2	ß	T	p	VIF	ANOVA
Perceived usefulness (PU)	Health safety in general	38.3%	0.4	4.6	$p \leq 0.001$	1.7	F (3,85)= 19.2, $p \leq 0.001$
	Quicker data access		0.2	2.5	p = 0.014		
	Lacking System reliability		-0.2	-2.6	p = 0.012		
	Worry about permanent surveillance	19.2%	-0.4	-4.2	$p \leq 0.001$	1.3	F (2,73)= 9.9, $p \leq 0.001$
	Protection of intimacy		0.2	2.1	p = 0.042		

At this point we forego the regression analyses for the several respondents groups (age, gender, and health status groups) because of the preliminary detailed descriptive analysis. Concluding the result section we can now state, which of the analyzed aspects of perceived security and privacy mostly contribute to the variance explanation of acceptance in terms of perceived usefulness of E-health technologies, and how the perception of these varies with respect to the user diversity. Short summary of the results is given below and discussed regarding advantages and possible barriers related to these facts.

V. DISCUSSION

The support of E-health technologies in populations getting older and older could facilitate the everyday life as well as maintain independency and mobility of persons with frail health. The challenge is not longer exclusively the technical feasibility and legal issues but rather the question, who expects what, and, how willingly the intended audience would use the technical assistance. The more strongly users' cognitions and mindsets are addressed and included into a sensitive communication and information concept, the higher is the chance of a broad user acceptance and the adoption of new medical technology. Thus, it is a matter of user acceptance, which determines the usage behavior and the broadening of medical technologies in private households.

However, health and aging are very sensible topics, and people deal with them in different ways. What is generally approved for illness or poor health, is the doctor-patient confidentiality as well as an overall discretion and protection of the privacy sphere of person concerned. Also, persons require security (i.e. invulnerability to external attacks) and seek for safety (i.e. protection from harm) for entire life, because these pertain to humans' fundamental needs. Hence, these

characteristics might be also crucial to assistive E-health technologies surrounding one in his/her own home environment.

The result of the present study showed that security and privacy aspects play an important role for diverse (potential) E-health technology users, and that there are some differences in the opinions, which need to be considered when aspiring high usefulness.

Regarding age, different perceptions of system security and data protection were found. In concrete terms: younger respondents stronger than middle-aged and older adults require high reliability for using E-health technology, and, with respect to data protection, there are high levels demanded in almost all age groups apart from the oldest one (70+years olds). These outcomes may be interpreted in two respects: first is, that older persons – as it is well known from the corresponding literature (e.g., [15], [18], [19]) – have less technical expertise, and as a result they might be less aware of the consequences of an insufficient and suboptimal system and data security; the second is, that they simply prioritize in different way than younger users do (i.e. for the older adults health maintenance is much more important than data protection). Either way, as far as these security aspects are concerned, there are statutory standards, which must be obeyed by developers and services. In addition, there are not meaningful differences about the privacy requirements in various ages. Much more persons in all age groups assign quite high relevance to privacy aspects.

Regarding gender, the analyses revealed significant differences with respect to data protection and access control. Women require higher security features in this regard than men. However, the male part of the sample perceive regular health monitoring by means of medical devices marginally as more beneficial in comparison to females. Considering this, again, it is conceivable that the technical know-how and experience, which are commonly higher in males (e.g., [7], [20], [21], [22]), may influence the opinions about the security in the particular gender groups. However, this explanation may not apply to differences in opinions about anonymity and intimacy in E-health usage context. These characteristics of privacy are esteemed higher in the female part of the population. Apparently, in this gender group the unobtrusiveness is a highly valued prerequisite of E-health technology usage, which nowadays – in times of Microsystems technologies – might be a very minor issue.

The most differences with respect to security and privacy, though, result concerning the (subjective perceived) health condition. In the area of security relevant differences emerge especially for general protection and self-determination of data transfer and storage. Here, healthy people pay more attention to data security than those with (chronically) diseases or frail health. Also, most privacy aspects are understood in different ways in individuals standing on the opposing poles of the physical condition scale: persons suffering from poor health do not insist on safeguarding of their private sphere, and they don't worry about continuous surveillance – quite the contrary to the healthy people. In this context, indeed, the prioritization of the own health could be a conceivable reason to estimate the relevance of some privacy aspects rather lower. It is understandable too, that sickly persons are rather willing to make their course of disease or the monitored vital parameters transparent and easily accessible, in order to facilitate the work of healthcare professionals. In contrast, respondents with (very) good physical condition pay decidedly more attention to privacy attributes like intimacy, anonymity, discreetness, and invisibility to others. Supposable, it is a part of human nature just to assert his right to privacy, because in those individuals, truly, there is neither physical nor emotional need to disclose such sensitive data.

But, which relevance have all these considerations for users acceptance and therefore for development and optimizing of E-health assistance? When analyzing the effects of all in this research regarded security and privacy aspects on perceived usefulness by means of multiple analysis of variance, perceived security reveals to be a major driver of acceptance ($F(33,231) = 1.9$, $p = 0.003$) but also privacy issues – even though to a lesser extent in comparison to security ($F(30,192) = 1.4$, $p = 0.084$). However, these outcomes provide insufficient information about the impact of the several characteristics. For this reason multiple regression analyses were undertaken in order to find out, which of the security and privacy attributes have the most powerful predictive power for the as useful perceived E-health technology. According to the statistics there are three security attributes, which explain almost forty per cent of the variance, i.e. the general safety feeling and quicker health data access in case of emergency, as well as inversely related lacking system reliability. Moreover, two privacy aspects contribute to the variance explanation of perceived usefulness of E-health technology: inverse directed worry about the permanent surveillance when monitoring some bodily functions, and, to a minor extend, the protection of intimacy. Due to these findings we can now give the empirical evidence for the fact, that the evaluated perceptions of privacy and security are significantly relevant parts of E-health technology acceptance, or – to be more precisely – to its perceived usefulness. Even though it is obvious, that the described security and privacy aspects are not the exclusive or primary factors which explain the acceptance, it is important to identify and understand those variables, as well as to determine the degree to which such concerns mediate acceptance in order to optimize and improve the subsequent usage of medical technologies.

To know, how people perceive the interaction and which relevance they attribute to security and privacy when using medical assistive systems, applications, or particular devices, paves the way to better usability, and in the consequence to a higher approval and usage increase. Thus, this research contributes to this knowledge in different ways. Firstly, it makes security, safety and privacy a subject of discussion and shows their importance as well as the mediating role for acceptance. Secondly, it performs statistical analyses to present to which degree those aspects are involved. Thirdly, the study additionally demonstrates, how diverse individuals perceive these characteristics or rather which differences exist regarding those in various groups of the population (with respect to age, gender, and health status).

Of course, there are also some limitations of the present study. Although these findings are informative, some methodological caution is still necessary. The results presented

here are based on a questionnaire method, of which we cannot for certain exclude some artificial findings. Not all persons participating came into direct contact with medical assistive devices, and thus, in order to answer some of the questions they had to envision this situation or answer in general. For sure, such respondents have entirely different background in comparison to diseased or chronically ill persons, who have day-to-day experience with this technology.

And also, the distribution of healthy participants and those with rather frail health condition for comparison of the opinions regarding security and privacy was not well balanced (20% poor health vs. 80% good health). In fact, it resulted from the randomly selection of the sample, but it still can lead to some under- or overestimations of the results. In addition, the analyses based on a self-reported current health state, where there was not a baseline given, so that the classifications can vary due to different perspectives of individuals (e.g., when a person refers a "good" health condition, but then declares to suffer from hypertension (= high blood pressure)). As regarding especially this user characteristic some real differences were to find, in future studies considerations need to be given to the composition of the sample in order to validate the here presented findings.

A final remark refers to the acceptance of medical assistance technologies. The outcomes in this study apply to only one part of acceptance (i.e. perceived usefulness), however, the construct itself – especially in medical context – is truly more complex, evincing dynamic components. Hence, the analyses and their interpretations must not be seen as exhaustive, but rather as a hint in this direction, which needs to be deepened further on.

Last but not least, following studies will have to investigate to what extent these outcomes may be generalized to other using contexts (e.g., acceptance as chronically ill person, as caregiver or family member, as somebody, who uses E-health in preventive way, etc.).

ACKNOWLEDGMENT

The authors would like to thank all focus groups and questionnaire participants for kindly communicate their opinions concerning the topics. We also thank Johanna Kluge for her supportive performance.

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

REFERENCES

[1] S. Lahlou, "Identity, social status, privacy and face-keeping in digital society", Social Science Information 47(3), pp. 299–330, 2008.

[2] E. M. Rogers, Diffusion of Innovations, 4th ed. New York, NY: The Free Press, 1995.

[3] S. Korupp, "No man is an island: The influence of knowledge, household settings, and social context on private computer use", International Journal of Internet Science 1, pp. 45–57, 2006.

[4] S. Meyer, H. Mollenkopf, „Home technology, smart homes, and the aging user", in K. W. Schaie, H.-W. Wahl, H. Mollenkopf and F. Oswald, Eds. Aging Independently: Living Arrangements and Mobility, Springer Publishers, 2003, pp. 148-161.

[5] M. Ziefle, and C. Röcker, „Acceptance of pervasive healthcare systems: a comparison of different implementation concepts." Full paper on the Workshop User-Centred-Design of Pervasive Health Applications (UCD-PH'10). 4th ICST Conference on Pervasive Computing Technologies for Healthcare 2010, 2010.

[6] S. D. Grabner-Kräuter, and E. A. Kaluscha, "Empirical research in on-line trust: a review and critical assessment". International Journal of Human-Computer Studies 58, pp. 783–812, 2003.

[7] W. Wilkowska, S. Gaul, and M. Ziefle, "A small but significant difference – the role of gender on the acceptance of medical assistive technologies", in G. Leitner, M. Hitz and A. Holzinger, Eds. HCI in Work & Learning, Life & Leisure, USAB 2010, LNCS 6389, Berlin, Heidelberg: Springer, 2010, pp. 82–100.

[8] K. E. Caine, A. D. Fisk, and W. A. Rogers, „Benefits and privacy concerns of a home equipped with a visual sensing system: a perspective from older adults". Proc. Human Factors & Ergonomics Soc., pp. 180-184, 2006.

[9] C. L. Corritore, B. Kracher, S. Wiedenback, and R. Marble, "Foundations for trust for E-Health", in M. Ziefle and C. Röcker, Eds. Emerging healthcare systems, Hershey, P.A. IGI Global, 2011, pp. 49-75.

[10] E. Montague, B. M. Kleiner, and W. W. Winchester, „Empirically understanding trust in medical technology". International Journal of Industrial Ergonomics 39(4), pp. 628-634, 2009.

[11] M. Petković, and L. Ibraimi, "Privacy and security in e-Health applications", in M. Ziefle and C. Röcker, Eds. E-Health, Assistive Technologies and Applications for Assisted Living: Challenges and Solutions, Hershey, P.A. IGI Global, 2011, pp. 23-48.

[12] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: toward unified view," MIS Quarterly, 27 (3), pp. 426-478, 2003.

[13] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology". MIS Quarterly 13, pp. 319-337, 1989.

[14] V. Venkatesh, and F. D. Davis, „A theoretical extension of the Technology Acceptance Model: four longitudinal field studies". Management Science 46, pp. 186-204, 2000.

[15] M. Ziefle, „Age perspectives on the usefulness on e-health applications", International Conference on Health Care Systems, Ergonomics, and Patient Safety (HEPS), Straßbourg, France, 2008.

[16] K. Arning, and M. Ziefle, „Different perspectives on technology acceptance: the role of technology type and age", in A. Holzinger and K. Miesenberger, Eds. Human – Computer Interaction for eInclusion. LNCS 5889, Berlin, Heidelberg: Springer, 2009, pp. 20-41.

[17] T. L. Mitzner, J. B. Boron, C. B. Fausset, A. E. Adams , N. Charness, S. J. Czaja, K. Dijkstra, A. D. Fisk, W. A. Rogers, and J. Sharit, "Older adults talk technology: technology usage and attitudes", Computers in Human Behavior 26, pp. 1710–1721, 2010.

[18] M. Ziefle, and A. K. Schaar, "Technical expertise and its influence on the acceptance of future medical technologies. What is influencing what to which extent?", in G. Leitner, M. Hitz and A. Holzinger, Eds. HCI in Work & Learning, Life & Leisure, USAB 2010, LNCS 6389, Berlin, Heidelberg: Springer, 2010, pp. 513-529.

[19] W. Wilkowska, and M. Ziefle, „Which factors form older adults' acceptance of mobile information and communication technologies?", in A. Holzinger and K. Miesenberger, Eds. Human – Computer Interaction for eInclusion, Berlin, Heidelberg: Springer, 2009, pp. 81-101.

[20] S. Gaul, W. Wilkowska, and M. Ziefle, „Accounting for user diversity in the acceptance of medical assistive technologies". Full paper at the 3rd International ICST Conference on Electronic Healthcare for the 21st century, eHealth 2010, 2010.

[21] P. Schumacher, and J. Morahan-Martin, "Gender, internet and computer attitudes and experiences", Computers in Human Behavior 17, pp. 95-110, 2001.

[22] M. R. M Meelissen, and M. Drent, „Gender differences in computer attitudes: does the school matter?", Computers in Human Behavior 24(3), pp. 969-985, 2008.